INDEX

Volume – I

(from page No 1 – 201)

SL NO.	PARTICULARS	PAGES
1.	**REJOINDER AFFIDAVIT ON BEHALF OF THE PETITIONER**	1 - 100
2.	**ANNEXURE - RA/1 (Part –I)** True photocopy along with typed copy of the relevant portion of the Oxford Pro Bono Publico submission dated Feb. 2013.	101 - 201

Continued Volume - II

(From pages 202 – 318)

1

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. 37 OF 2015

IN THE MATTER OF:

Mathew Thomas ...Petitioner

Versus

Union of India & Ors .... Respondents

REJOINDER AFFIDAVIT ON BEHALF OF THE PETITIONER

I, Mathew Thomas, son of Late T.P.John, R/o No.18-A, Adarsh Vista, Basavanagar, Bangalore-560037, Karnataka, presently at present at New Delhi, do solemnly affirm on oath and state as under:-

1. I am the Petitioner in the instant Writ Petition and I am well versed with facts of the present case and I am, therefore, competent to swear and sign the present affidavit.

2. I have gone through the contents of the Counter Affidavit filed by Respondent Nos.1-7 and the instant Rejoinder Affidavit is being filed in reply thereto.

PARAWISE REPLY

3. That the contents of para 1 of the Counter Affidavit are formal in nature and therefore do not call for response.

4. That the contents of para 2 of the Counter Affidavit do not call for reply. It is however necessary to say that while all efforts have been made to reply to each and every aspect raised in the Counter Affidavit, nothing not specifically dealt with may be being admitted merely for non-traverse.

5. That the contents of para 3 of the Counter Affidavit to the extent it relates to Article 21 are not in dispute. It is reiterated that collection of personal data, which is disproportionate and lacks nexus with the object sought to be achieved violates fundamental rights of the citizens of India. In this paragraph, it is now an admitted position that the purpose of UID is to provide an identity, allegedly for delivery of services. The Petitioner reiterates that there are various other identity proofs available which can well be used for delivery of services and collection of biometric data is not relevant to delivery of services.

6. That the contents of para 4 of the Counter Affidavit is formal in nature and does not call for any reply. It is however denied that the Writ Petition is misconceived in law and facts.

REPLY ON THE ISSUE OF MAINTAINABILITY AND ENTITLEMENT TO RELIEF

7. That the contents of para 5 of the Counter Affidavit are denied except in so far as it relates to matters of record. It is submitted that there is no delay whatsoever as alleged or otherwise. The Petitioner has exhausted all proper remedies before approaching this Hon'ble Supreme Court.It is important to reassert that the UID scheme has not been authorised by the Legislature, and unless there is a statutory empowerment in accordance with the Constitution, collection

of personal data is impermissible under the Constitution. It is also relevant to submit that the validity of Aadhar has been sub judice since 2012 and various representations have been moved by persons prior to that. However, the Respondents have proceeded in collection of data and increasing the penetration of Aadhaar without first making any attempt to have the matter adjudicated by this Hon'ble Court. Further, the Petitioner had filed a Civil Suit being OS No.8181 of 2012 before City Civil Court, Bangalore against UID and Planning Commission and had been pursuing the said remedy in good faith.

8. That the contents of para 6 of the Counter Affidavit are denied as being untenable. It is denied that the UID scheme is at its peak. It is also denied that enrolment for UID is voluntary. The Respondents have adopted various means and mechanisms to quietly and surreptitiously make enrolment for Aadhaar mandatory and compulsory without passing any such express orders to overcome the interim orders passed by this Hon'ble Court.Since the UID scheme is itself invalid and impermissible under the Constitution, any amount of money spent on it cannot make it permissible. Merely because the Respondent has incurred expenditure (which it ought not to have because the matter was sub judice) would not result in creation of any equity in favour of the Respondents. If the scheme is invalid under the Constitution, it would have to be held so without regard to the money having been spent on it. The price that the citizens of this country have paid for freedom and organising themselves under the Constitution is way too much to be jeopardised merely because Respondent No.1 has incurred

expenditure in promulgation and penetration of a constitutionally impermissible scheme.

9. That the contents of para 7 of the Counter Affidavit are denied as being incorrectly stated. The UID scheme itself does not constitute a welfare scheme; and is incapable of uplifting the lower strata of the society as alleged. The various welfare schemes of the Central and the State Governments are capable of otherwise coming to the rescue of such section of the society. It is reiterated that the difficulties in implementation of the said social schemes is not on account of identification of an individual, but identification of a class that would be entitled to the said schemes. In other words, the problem is wholly of incorrect definitions, untenable exclusions, and erroneous inclusions – which are not related to individual's identities. It is denied that the Petitioner has come at a belated stage. The Petitioner is advised to say that the reliance by Respondent No.1 on *Narmada Bachao Andolan v. Union of India* (2000) 10 SCC 664 para 45-48 is untenable. The said case was for construction of a dam which affected large number of persons, but had nothing to do with collection of biometrics, and retina details on an ongoing basis State. Similarly, reliance on *Raunaq International* (1999) 1 SCC 492 is misplaced.

10. That the contents of para 8 of the Counter Affidavit are not disputed to the extent they relate to matters of record. It is submitted that the Petitioner has made full disclosure of the pending impleadment application. It is also pertinent to add here that the impleadment application has still not been allowed by this Court.

11. That the contents of para 9 of the Counter Affidavit are denied as being incorrectly stated. In fact, the Civil Suit OS No.8181/2012 was dismissed by the City Civil Court inter alia on the ground that the Petitioner has raised constitutional issues which cannot be considered by a Civil Court and yet a cost of Rs.50,000/- was imposed. The said order is under challenge in Regular First Appeal. The Petitioner has made appropriate disclosures in this regard. It is denied that Petitioner has filed the present Writ Petition to circumvent the payment of costs, which is under challenge before appropriate Court. It is denied that there is any abuse of process by the Petitioner.

12. That the contents of para 10 of the Counter Affidavit are denied as stated and it is submitted that the Respondents are reading the contents of First Appeal outside the context in which they are written. The rejection of the Suit No.8181/2012 was pursuant to the application under Order VIII Rule 2. It is submitted that it is completely contrary to the settled law for a Court of Law to reject a plaint on the ground that it raises issues that touch upon the Constitution. Therefore, the RFA before the High Court raises said substantive questions of law. It is in the fitness of things that when the Supreme Court of India is seisin of the matter, the question of validity of UID scheme be heard by this Court alone. It is also denied that the RFA is presently pending before the Karnataka High Court. It has since been withdrawn by the Petitioner and accordingly dismissed as withdrawn.The deponent has requested his advocates to apply for a certified copy of this order.

13. That the contents of para 11 of the Counter Affidavit are denied as stated. It is submitted that the fact that the order of the Trial Court has been stayed is something in favour of the Petitioner. Further, the Respondent has not established as to how the alleged non-disclosure of the said stay order prejudices the instant Writ Petition.

14. That the contents of para 12 of the Counter Affidavit are denied as stated. It is submitted that the Petitioner's Suit No.8181/2012 has been dismissed at a preliminary stage, and therefore the issue of res judicata is not applicable as is sought to be suggested by the Respondents.

15. That the contents of paras 13 and 14 of the Counter Affidavit are denied. It is submitted that the order dated 30.4.2014 does not dispose of the Contempt Petition No.144/2014 but only disposes of the I.A. No.1 of 2014 filed in the said Contempt Petition on the basis of assurance given by the Ld. Solicitor General.

16. That the contents of para 14 of the Counter Affidavit are denied as being incorrectly stated except in so far as it relates matters of record. It is submitted that the Writ Petition had been filed before the Delhi High Court which arises out of denial of information to the Petitioner by UID in so far as the Petitioner is seeking information with respect to MNC. In fact, at page 89 of the Writ Petition, the Petitioner has stated that it is the obligation of the Respondents to bring on record the documents/contracts between UID and MNC contractors, however, apart from trying to scuttle the proceedings by adverting to the Delhi High Court proceedings, the Respondent has not brought any material

before this Hon'ble Court and has only stated that it has complied with the order passed by the CIC. The Petitioner has stated in the Writ Petition itself that the reply which has been received from CIC is incomplete. Thus, the Petitioner has made adequate disclosure which is germane and necessary for the proceedings before this Hon'ble Court. Further, the matter before the Delhi High Court relates to violation of provisions of the Right to Information Act by the respondents and not the legality of the Aadhaar scheme.

17. That the contents of para 15 of the Counter Affidavit are denied as wrongly stated and it is submitted that the Writ Petition is maintainable. The Petitioner strongly contests the allegation of forum shopping and bench hunting. None of the grounds taken by the Respondent disentitles the Petitioner from relief from this Hon'ble Court.

REPLY TO ALLEGATIONS OF LOCUS STANDI OF THE PETITIONER

18. That the contents of para 18 of the Counter Affidavit are denied as stated. However, it is to be noted that it is admitted position that UID scheme claims to provide identity.

Note: Paragraphs 16 is wrongly numbered as paragraph 18. However, the Rejoinder has been prepared keeping in mind the paragraph numbers given in the Counter even though they are incorrectly numbered, for the sake of convenience.

19. That the contents of para 19 of the Counter Affidavit are denied as wrongly stated and it is submitted that as a citizen of India, Petitioner has every right to challenge the UID scheme. The Petitioner has not enrolled for UID as doing the same not only harms his fundamental right but also since it

may be construed as waiver to challenge the same. It is denied that the enrolment in Aadhaar is voluntary and with informed consent. The Petitioner has come across many individuals who have enrolled in Aadhaar only because availing of essential services had been linked to Aadhar. Therefore, the Petitioner submits that the "informed consent" of the masses for availing the Aadhaar card in many instances is only for the purpose of availing essential services for which the Respondent has made the possession of an Aadhaar card a compulsory pre-condition. It is submitted that the entire generation of UID number is upto the Respondents and they may generate as many Aadhaar numbers as they may wish, however, not all the residents have been provided with UID number and therefore the Writ Petition is maintainable and the Petitioner is entitled to relief. The para under reply is vague in as much as it does not specify as to how poorer and weaker sections are benefited merely by having UID number and as to how other methods of proving identity are not workable. The Petitioner submits that the entire expense of over Rs.5000 crores on UID could have been avoided as the country did not need another identity proof.

20. That the contents of para 20 of the Counter Affidavit are incorrectly stated and are denied; and in fact, throughout the Writ Petition the Petitioner has established violation of fundamental rights invoking the jurisdiction of this Hon'ble Court under Article 32 of the Constitution.

21. That the contents of para 21 of the Counter Affidavit are denied as stated and it is submitted that they are based on incorrect understanding of "public interest litigation" and

cognate jurisdiction of this Hon'ble Court. It is denied that the majority population of India is capable of voicing its concerns as alleged. In fact, majority of the population in India, mostly living in villages and small towns is incapable of approaching the Courts of Law, and therefore the jurisdiction of this Court had been expanded by relaxing the rules of locus standi. Hence, the Petitioner does have the locus standi to approach this Hon'ble Court on behalf of the citizens of this country whose fundamental rights are sought to be abridged by the Respondents. It is denied that the instant Writ Petition is based on "purely hypothetical scenarios".

22. That the contents of para 22 of the Counter Affidavit are denied as stated and in response it is stated that the Writ Petition does not seek to raise "simply issues of policy". The issues raised in the instant Writ Petition are grave constitutional issues. The Petitioner as a citizen of India – a republic limited by the Constitution, is entitled to approach the Court of Law to enforce the letter and spirit of the Constitution and to seek accountability from the Respondents. What has been projected as a "policy of identification" is actually a scheme to identify and segregate individuals and collect their private data, and personal profiles giving rise to a surveillance State. The purported "policy of identification" has a direct impact on fundamental rights of individuals and in the garb of a "policy decision", fundamental and legal rights of citizens cannot be abridged. Further, identification as alleged also relates to a relationship between Citizen and the State, and therefore, the moment State wishes to identify citizens, it ceases to be a policy

decision, and necessarily needs to be permitted, controlled and regulated by a law, as only Parliament by law can abridge fundamental rights and human rights.

The Petitioner submits in this regard that the fundamental rights of citizens cannot be infringed by the state taking shelter under any policy. The executive power of the State cannot be extended to impose restrictions on fundamental rights, and every act done by the State must if it is to operate to prejudice any person be supported by legislative authority. In view of this, in the case of Kharak Singh v State of Punjab, 1964 (1) SCR 332 a six judge bench of this hon'ble Court held that:

> **5.** Before entering on the details of these regulations it is necessary to point out that the defence of the State in support of their validity is two-fold: (*1*) that the impugned regulations do not constitute an infringement of any of the freedoms guaranteed by Part III of the Constitution which are invoked by the petitioner, and (*2*) that even if they were, they have been framed "in the interests of the general public and public order" and to enable the police to discharge its duties in a more efficient manner and were therefore "reasonable restrictions" on that freedom. *Pausing here it is necessary to point out that the second point urged is without any legal basis for if the petitioner were able to establish that the impugned regulations constitute an infringement of any of the freedoms guaranteed to him by the Constitution then the only manner in which this violation of the fundamental right could be defended would be by justifying the impugned action by reference*

> *to a valid law i.e. be it a statute, a statutory rule or a statutory regulation.* Though learned Counsel for the respondent started by attempting such a justification by invoking Section 12 of the Indian Police Act he gave this up and conceded that the regulations contained in Chapter 22 had no such statutory basis but were merely executive or departmental instructions framed for the guidance of the police officeRs They would not therefore be "a law" which the State is entitled to make under the relevant clauses 2 to 6 of Article 19 in order to regulate or curtail fundamental rights guaranteed by the several sub-clauses of Article 19(1), nor would the same be "a procedure established by law" within Article 21. The position therefore is that if the action of the police which is the arm of the executive of the State is found to infringe any of the freedoms guaranteed to the petitioner would be entitled to the relief of mandamus which he seeks, to restrain the State from taking action under the regulations.

The Petitioner further submits that in the case of *Ramlila Maidan incident, In Re*, it has been clearly held by this Hon'ble Court that:

> **29.** Now, I would examine the various tests that have been applied over the period of time to examine the validity and/or reasonability of the restrictions imposed upon the rights.
>
> **30.** No person can be divested of his fundamental rights. They are incapable of being taken away or abridged. All that the State can do, by exercise of its legislative power, is to regulate these rights by

imposition of reasonable restrictions on them. Upon an analysis of the law, the following tests emerge:

(a) The restriction can be imposed only by or under the authority of law. It cannot be imposed by exercise of executive power without any law to back it up.

(b) Each restriction must be reasonable.

(c) A restriction must be related to the purpose mentioned in Article 19(2).

The questions before the Court, thus, are whether the restriction imposed was reasonable and whether the purported purpose of the same squarely fell within the relevant clauses discussed above.

Note: In the Counter Affidavit, paragraphs 23 to 26 are missing. Therefore the next para starts from para 27.

ON THE ISSUE OF CONSTITUTIONAL AND LEGAL BASIS OF UNIQUE IDENTIFICATION SCHEME

23. That the contents of para 27 of the Counter Affidavit are denied as stated as the same is based on incorrect understanding of Article 73 of the Constitution of India. There cannot be any iota of doubt that the collection of personal information and rendering the UID number as virtually mandatory can only be done pursuant to legislative authority. In the present case, notwithstanding the scope of Article 73 which is co-extensive with Schedule VII, the collection of personal information cannot be authorised by executive order that too issued in favour of an authority which is not accountable to the Legislature. Article 73 begins with the phrase "*subject to the provisions of this*

Constitution" and, therefore, Article 73 does not give the Executive an absolute power to do anything which falls under List I of Schedule VII. The cases of *Kharak Singh v. State of Punjab* and *Ramlila Maidan Incident, In Re* (Supra) substantiates the same.

24. That the contents of para 28 of the Counter Affidavit are denied as stated. In response, it is submitted that the Respondents have admitted that "*UID scheme is relatable to the basic fundamental right....*" and therefore, it naturally follows that a scheme that is relatable to the basic fundamental right and abridges or in any way impinges on it, is required to be legislatively authorised. The notification dated 28.1.2009 is itself ultra vires the Constitution as it seeks to create an authority which is not 'accountable' to the Legislature, a methodology not contemplated under the Constitution. The said notification further vests the ownership of UID database with the UIDAI/Respondent No.3 which is impermissible as all properties have to be held by the President of India. Further, Respondent No.3 is also not a body corporate under any statute, and naturally cannot contract or hold properties. The said notification does not even authorise collection of biometric, but only creates an authority that has to issue unique identification documents. Thus, the notification is excessive delegation of even the limited powers, which are traceable to Art 73. Even any method or procedure has not been prescribed by the said notification.

The Petitioner emphatically denies that no further law is necessary for operation of the UID scheme as has been stated by the Respondent. The question of whether the

executive can intefeare with fundamental rights merely because the State has power to legislate on the said subject is no longer res integra. This issue was considered in the case of *State of Madhya Pradesh v. Thakur Bharat Singh,* 1967 (2) SCR 454 where it was held:

> **6.** Counsel for the State relied upon the terms of Article 162 of the Constitution, and the decision of this Court in *Rai Sahib Ram Jawaya Kapur* v. *State of Punjab* [(1955) 2 SCR 225] in support of the contention that it is open to the State to issue executive orders even if there is no legislation in support thereof provided the State could legislate on the subject in respect of which action is taken Article 162 provides that subject to the provisions of the Constitution, the executive power of a State shall extend to the matters with respect to which the Legislature of the State has power to make laws. But Article 162 and Article 73 are concerned primarily with the distribution of executive power between the Union on the one hand and the States on the other, and not with the validity of its exercise. Counsel for the State however strongly relied upon the observations of Mukherjea, C.J., in *Rai Sahib Ram Jawaya Kapur's case* [(1955) 2 SCR 225] :
>
> > "They do not mean, ... that it is only when the Parliament or the State Legislature has legislated on certain items appertaining to their respective lists, that the Union or the State executive, as the case may be, can proceed to function in respect to them. On the other hand, the language of Article 162 clearly indicates that the powers of

> the State executive do extend to matters upon which the State Legislature is competent to legislate and are not confined to matters over which legislation has been passed already."

These observations must be read in the light of the facts of the case. The executive action which was upheld in that case was, it is true, not supported by legislation, but it did not operate to the prejudice of any citizen. In the State of Punjab prior to 1950 the text books used in recognized schools were prepared by private publishers and they were submitted for approval of the Government. In 1950 the State Government published text books in certain subjects, and in other subjects the State Government approved textbooks submitted by publishers and authors. In 1952 a notification was issued by the Government inviting only "authors and others" to submit textbooks for approval by the Government. Under agreements with the authors and others the copyright in the text books vested absolutely in the State and the authors and others received royalty on the sale of those text books. The petitioners — a firm carrying on the business of preparing, printing, publishing and selling text books — then moved this Court under Article 32 of the Constitution praying for writs of mandamus directing the Punjab Government to withdraw the notifications of 1950 and 1952 on the ground that they contravened the fundamental rights of the petitioners guaranteed under the Constitution. It was held by this Court that the action of Government did not amount to infraction of the guarantee under Article 19(1)(*g*) of the

Constitution, since no fundamental rights of the petitioners were violated by the notifications and the acts of the executive Government done in furtherance of their policy of nationalisation of text books for students. It is true that the dispute arose before the Constitution (Seventh Amendment) Act, 1956, amending inter alia, Article 298 was enacted, and there was no legislation authorizing the State Government to enter the field of business of printing, publishing and selling text books. It was contended in support of the petition in *Rai Sahib Ram Jawaya case* [(1955) 2 SCR 225] that without legislative authority the Government of the Slate could not enter the business of printing, publishing and selling text books. The Court held that by the action of the Government no rights of the petitioners were infringed, since a mere chance or prospect of having particular customers cannot be said to be a right to property or to any interest or undertaking. It is clear that the State of Punjab had done no act which infringed a right of any citizen: the State had merely entered upon a trading venture. By entering into competition with the citizens, it did not infringe their rights. *Viewed in the light of these facts the observations relied upon do not support the contention that the State or its officers may in exercise of executive authority infringe the rights of the citizens merely because the Legislature of the State has the power to legislate in regard to the subject on which the executive order is issued."*

25. That the contents of para 29 of the Counter Affidavit are denied and it is submitted that a legislation for the purposes of execution of the UID scheme is an absolute minimum under the Constitution. It is settled law that specific legislation may indeed be necessary if the Government require certain powers in addition to what they possess under ordinary law in order to carry on the particular trade or business. Thus when it is necessary to encroach upon private rights in order to enable the Government to carry on their business, a specific legislation sanctioning such course would have to be passed.(*Ram Jawaya Kapur v. State of Punjab*, AIR 1955 SC 549). The decision of Kerala High Court reported at AIR 1958 KER 290 also has no bearing in the present case as in the said case the Legislature had already considered and passed the legislation concerned. However, in the present case, there are various reports of the Standing Committee rejecting the UID scheme in the present form, and despite that, Respondent No.1 while overlooking the Parliamentary checks and balances is proceeding with the UID scheme.

26. That the contents of para 30 of the Counter Affidavit are denied as stated and it is submitted that the fetters on the power of the executive, in the present case, have been imposed by the Constitution itself. Therefore, the executive is acting contrary to the Constitution in proceeding with the UID scheme while affecting fundamental rights. It is submitted that once the Respondents have already prepared a draft Bill which they themselves feel is necessary in the constitutional scheme, it is not open to the Respondents to

proceed with the UID scheme without first getting the Bill passed in both Houses and assented to by the President.

27. That the contents of para 31 of the Counter Affidavit are denied as stated. It is submitted that the averments are vague in that they do not explain as to how provision of UID number itself is going to ensure delivery of benefits to the poorer sections. It is submitted that doctrine of proportionality requires the Government to consider whether the same objective can be achieved by any other less intrusive means, and in the present case even in the absence of UID number, by identifying bank account number (along with IFSC code) straightaway payment can be made to the account by the Government without the need for any intermediate identification document including Aadhar. In any case, if the object as stated by the Respondent is to overcome the problem that the benefits of social welfare schemes were "not reaching to a large number of people primilarly the poorest and most deserving, at the bottom of the pyramid for want of being able to prove their identity to service providers and agencies which dispense such benefits", there is no intelligble nexus as to why the UID number must be made compulsory for marriage registration, payment of salaries of government employees etc. Therefore, UID number is nothing but another identity card, in this regard made available to the people under the label of it being something novel and motivated towards fulfilment of social welfare policy.

RIGHT TO IDENTITY AS A FUNDAMENTAL RIGHT

28. That the contents of para 32 of the Counter Affidavit are denied. It is submitted that the respondents' misconception of the human right to be recognized as human beings as a right to identity and hence, by implication, to be identified by authorities, is perverse and untenable.

29. That the contents of para 33 of the Counter Affidavit are denied except in so far as it seeks to suggest that right to identity is a fundamental right. However, it is submitted that 'right to identity' through Aadhar/UID' is not a fundamental right and the Government cannot insist upon collection of personal data in order to recognize its citizens or other persons residing within its territory. Article 6 of the Universal Declaration of Human Rights provides that "Everyone has the right to recognition everywhere as a person before the law."; and such right does not enable the Government to collect personal data more than is necessary to recognize a person before law. There is no material placed on record by the Respondents which establishes that the problem in delivery of welfare services is on account of lack of identity proof or duplication. Further, the extent of the problem has also not been identified by the Respondents appropriately. The Petitioner denies that the problem is account of the identification of the individual recipient/beneficiary. The problem if at all, is due to incorrect inclusion and exclusion of entitled individuals. For instance, the debate about below poverty line individuals is essentially of identification of the cut-off line and not about identifying those very individuals. In fact, Aadhaar card by itself does not indicate that a person is entitled to welfare scheme. Therefore, even with

Aadhaar card, genuinely entitled individuals may be excluded if the policy determining the basis of inclusion/exclusion is not correctly formulated. The alleged great boost to identity of a person is nothing but another identity provided to existing individuals. It is relevant to note that in order to enrol for Aadhaar, a person is required to possess identity proofs and residence proofs, which naturally means that the person already has identity documents and therefore, UID number is only an "additional identity proof". The Petitioner submits that the Respondent in the garb of fostering a Right to Identity, one which is already sufficiently provided for by the State, in the form of various identity proofs and documents, is abridging the Right to Life and Dignity of individuals through the Aadhaar scheme. It is reiterated that the right of a human being is to be recognized as a person under law, and there is Right to Recognition and not Right to Identity.

30. That the contents of para 34 of the Counter Affidavit does not call for a reply. However, it must be stated that the Respondent's reliance on the UDHR to claim that the UID scheme furthers the right to identity is entirely misplaced. Article 12 of the UDHR guarantees the right to privacy of individuals. Such right can only be interfered with through a legislation as per Article 29(2) of the UDHR. Hence, contrary to this the Respondent's current scheme is in clear violation of the UDHR.

31. That the contents of para 35 of the Counter Affidavit are denied to the extent it seeks to suggest that a measure taken in purported fulfilment of obligations arising out of Article 21

of the Constitution can be beyond the pale of challenge. As stated above, UID number is an additional identity proof and no more. Even then, the Petitioner reiterates that the UID scheme is abridging other Rights under Article 21 such as the Right to Privacy of individuals. The Respondent while contending that the UID Scheme enriches the Right to identity under Article 21, has not only failed to demonstrate in what way such a right is enriched, but also failed to show how other rights guaranteed under Article 21 such as privacy rights are not infringed. It is vehemently denied that it is any defence to violation or abridgement of any fundamental right under the Constitution on the reasoning that the UID scheme provides an additional identity proof

REPLY IN RESPECT OF DUTY OF THE STATE TO IDENTIFY ITS RESIDENTS UNDER DIRECTIVE PRINCIPLES OF STATE POLICY

32. That the contents of para 36 of the Counter Affidavit are denied and in response it is stated that Article 38 relates only to securing social order for promotion of welfare of people and does not justify or contemplate a scheme to mandate collection of fingerprints and other personal details of every resident, especially since welfare schemes are capable of being executed without fingerprints. In fact, in a country like India where large number of people are manual labours whose fingerprints may be imperfect (or worn off due to manual/agricultural activities), such an approach would be counter-productive. Article 39(b), 39(c), 46, 47 and 51(c) does not in any way justify introduction of an extraordinary measure of collection of personal and vital details of residents of India, that too without legislative authority.

Further, the duty to respect international law and obligations oblige India to not collect and store personal data of its residents.

33. That the contents of para 37 of the Counter Affidavit are denied as stated and it is submitted that the same is based on incorrect premise and understanding of human rights jurisprudence. The argument raised in the para under reply is premised on incorrect basis that UID scheme itself is a welfare scheme which it is not. Even if one assumes that UID is only for the purposes of identification of the beneficiaries of welfare schemes, even then there are less disproportionate mechanisms available to identify the beneficiaries. As stated above, the problem is of errors in inclusion and exclusion and not an identification. To the extent the Respondents wish to eliminate wrong beneficiaries, it will have to begin with minimisation of corruption and commission widely infested in the public distribution system; which has got nothing to do with the UID scheme. For these reasons, amongst others, the UID scheme lacks rational nexus and is violative of Articles 14 and 21 of the Constitution of India. Prof. Sandra Fredman's book on "Human Rights Transformed" does not suggest that individual human right to privacy be trammelled in order to enforce so called welfare schemes. It is submitted that the contemporary approach in the UK and in the European Union is to apply doctrine of proportionality, which necessarily requires adjudging whether the object sought to be achieved matches with and is proportionate to the means used and whether a less intrusive means would have been used. In fact, Biometric Identification and Privacy: Comparative

Research Prepared for the Centre for Law and Policy Research, India, prepared by Oxford University's Oxford Pro Bono Publico in which special thanks has been given to Prof. Sandra Fredman for her "support and assistance for the project", notes that UID "if completed, this will be world's largest biometric database. However, India currently lacks comprehensive data privacy protection laws and the Draft National Identification of Authority Bill, 2010 contains limited safeguards". True photocopy along with typed copy of the relevant portion of the Oxford Pro Bono Publico submission dated Feb. 2013. is annexed herewith and marked as **Annexure – RA/1** (Page 181 - 429)

It is further submitted that UID scheme does not ensure data security and it lacks any framework of protection of data. It is denied that the present state of privacy laws as developed by Courts in India under doctrine of stare decisis is capable of affording protection to an individual as is expected under a data protection legislation through data controllers. It is further denied that provisions of IT Act are capable of protection to individuals who have been forced to submit their personal details to UIDAI.

34. That the contents of para 38 of the Counter Affidavit are denied. It is submitted that the UID scheme is not traceable to any of the Directive Principles of the State Policy, and in any event, the directives can never override fundamental rights but have to be only in aid of fundamental rights.

35. That the contents of para 39 of the Counter Affidavit are denied as being falsely stated. There is no statutory backing of UID scheme. It is denied that the identity programmes in

other countries as suggested are "similar", and in any event, the programme in other countries are authorised by statute and are also protected by data protection legislations which is lacking in India.

REPLY TO RIGHT TO IDENTITY AND NOT TO CITIZENSHIP

36. That the contents of para 40 of the Counter Affidavit are denied as stated. The Petitioner takes strong objection to the use of the word 'service' in relation to essential governmental functions. It is submitted that even in absence of UID number welfare schemes are capable of being administering equally well. The inability of the Government to contain and arrest corruption cannot be the basis for mandating collection of fingerprint, photograph and iris scan along with other personal details. It is submitted that merely through UID number "ineligible beneficiaries" cannot be weeded out in as much as eligibility is a function of definition determined by the Government and not the identity of a person. To the extent a person is to be identified, the present scheme and methods are more than sufficient not warranting any further intrusion by the Government.

37. That the contents of para 41 of the Counter Affidavit are denied except in so far as it relates to matters of record. It is stated that National Register for Indian Citizens is different from National Population Register, as the former is for citizens and the latter is for residents. The Citizenship Act permits only National Register for Indian Citizens and not National Population Register. Therefore, enrolment of Aadhaar for the National Population Register is also legislatively im permissible. It is relevant to note that the

NPR form contains field for "nationality as declared" – implying that there is no prior search or basis for determining citizenship of an individual before entering his name into the NPR. It is submitted that even the Government categorically claims that NPR is first step of NoRIC. It is submitted that all persons enrolling for Aadhar are automatically put in the database of the National Population Register without their consent; and even when people are enrolled for Aadhar, they are told that the same is mandatory in order to avail essential amenities provided by Government including the securing of driving license, registration of documents done under the Registration Act etc. It is denied that 1933 Montevideo Convention contemplates that the States will collect personal and private information including the biometric information of a person.

38. That the contents of para 42 of the Counter Affidavit are denied. It is reiterated that Section 14A of the Citizenship Act is ultra vires the Constitution in as much as it permits enrolment into the NPR (equal to NoRIC as the present approach discloses) of non-citizens without fulfilling the mandatory criterion of citizenship.

39. That the contents of paras 43 and 44 of the Counter Affidavit are denied as stated and it is submitted that contents of paragraph 43 itself demonstrate that what Section 14A contemplates is a register of citizens and not a register of residents. Therefore, to make a register of residents itself is beyond the statute. The problem of illegal immigrants prevailing in the border areas cannot be contained merely by register of residents and therefore the UID lacks vision and rational nexus.

REPLY TO RIGHT TO PRIVACY AND DATA PROTECTION

40. That the contents of para 45 of the Counter Affidavit are denied as stated and in response it is submitted that as under:-

(i) The legislative provision contained in the Information Technology Act, 2000 is incapable of checking leakage of data and biometric details of individuals. Simply by the process of criminalising of conduct, the personal and private information of individuals cannot be protected. A data protection legislation would require more than this.

(ii) It is denied that UID scheme contemplates sufficient mechanism to prevent data security. It is reiterated that the contractors engaged for this purpose, are themselves tainted and are controlled by foreign hands. As set out in the Writ Petition, the credentials of the contractors are doubtful and hence any amount of processes deployed by UID itself cannot ipso facto guarantee the safety of data. Furthermore, in the contract with L1 solutions annexed it is categorically mentioned that the company L1 India was established solely for the purpose of signing the contract. Therefore the respondent's stand here and elsewhere in the counter that no foreign entity is being engaged in the collection and aggregation of data is entirely false. The company is in effect between UIDAI and a US company. Infact most of the terms of the contract make reference to a US company and not its Indian subsidiary. For instance clause 19.4 of the

contract refers to the fact that the company must obtain all requisite permissions and licenses and fulfil all its legal obligations. However the reference in this clause is the US Company and not L1 India. True photocopy along with typed copy of the relevant portion of the contract dated nil entered between M/s L-1 identity solutions and UIDAI, dated 24.08.2010 is annexed herewith and marked as **Annexure RA/2 (page** 430 - 435]

(iii) Absence of a data protection legislation in India and a legislation that can protect privacy of an individual to the extent contemplated under the Constitution is a sine qua non for floating any kind of scheme to collect personal data. The Petitioner however maintains that even in such a situation where there is a data protection legislation, fingerprint and iris details cannot be taken, and stored remotely. In none of the countries to which reference has been made by the Respondents is the data stored or controlled remotely.

(iv) The contents of paragraph 45(iv) have been dealt with above and are not reiterated here.

41. That the contents of para 46 of the Counter Affidavit are denied and in response it is submitted that merely because the accounts of UIDAI are audited by the CAG or that UIDAI is subject to the Right to Information Act are not sufficient safeguards against absolute and arbitrary collection of information and making the same available to entities. It is reiterated that the Aadhaar scheme allows Respondents to

connect silos of information and thereby track everything done by an individual through a number generated by computer.

42. That the contents of paras 47 and 48 of the Counter Affidavit are denied. In response it is submitted that even though in theory Aadhaar number is verifiable as alleged, even then it has been rendered by the Government as a mere additional identity proof whose photocopies are readily accepted by the Government for proving the identity. The process of online verification in "cost effective manner" indicates that there is a commercial purpose beyond collection of personal information. In fact, recently UIDAI had called upon various mobile application developers to use Aadhaar platform to develop applications. It is submitted that given the large number of errors and fake Aadhar cards being issued to individuals, even this mechanism is not foolproof. It is submitted that it is not the number but the information that is attached to the number is capable of carrying individual's identity, especially when connected to other silos of information such as bank accounts, insurance, driving license etc. Further, the submission of the Respondent that the UID seeding is "strictly" a "one way linkage" stands inadequately proved. In the absence of any guidelines or legislation in this regard, the Petitioner submits that the UID scheme is open to great misuse of personal information of individuals.

43. That the contents of para 49 of the Counter Affidavit are denied and in response it is submitted that the administration of Aadhaar scheme is completely covered in secrecy and there is no public document that explains step by step software/mechanism that is deployed for the purposes of

Aadhaar, however, it is widely known that if Aadhaar number is "seeded" in every database, it is easy to access each and every activity of an individual through that UID number. It cannot be ruled out that the Government will not track individuals almost in real time. The petitioner also reiterates that there is a complete absence of guidelines or law to afford any protection in this regard.

It is further contended that the requirement of transparency is a pre-requisite in any governmental action which intrudes into the privacy of individuals. The European Communities Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data mandates that a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as the recipients or categories of recipients, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. In the present case, no such disclosure has been made to any citizen of India. Unless such information is made to the public through a legislature, any claim made by the Respondents regarding transparency would have to be deemed baseless.

44. That the contents of para 50 of the Counter Affidavit are denied and in response it is submitted that the consent of an individual given by enrolling for Aadhaar cannot be called free and informed consent. Individuals choosing to enrol for Aadhaar are compelled to do so on account of it having been made mandatory by various authorities. In absence of such a "whip" an individual may not even go to an Aadhaar camp. Further, even at enrolment camps, the issues of privacy are not sufficiently explained by the "enrolling agent" who is normally a private person to the individual enrolling for Aadhar. The alleged choice of residents is a farce choice and does not exist in reality. It is also denied that the residents have a choice to revise their choice subsequently, since there is no destruction of data guideline or the like available in the UID scheme.

45. That the contents of para 51 of the Counter Affidavit are denied. Further, it is submitted that the possibility of linking of various silos of information renders UID database into "monster database". It is denied that the scheme is in fact benefitting the poor segment of the population specifically. Although both the fingerprints and iris scans are being taken for biometric identification, the Direct Benefit transfer process undertaken by the Government for all schemes with cash transfers, the payment is being made through automated machine which only relies on the fingerprints of the persons. As highlighted in a news article in the Hindu, titled 'To pass biometric identification, apply Vaseline or boroplus on fingers overnight', a large number of persons belonging to the poor section of the society and engage in manual labour are unable to receive their pensions due the

non-recognition of their fingerprints by the micro-ATM machines. True photocopy along with typed copy of the relevant portion of the Article taken by the petitioner from the Newspaper 'The Hindu' dated 15.12.2012 is annexed herewith and marked as **Annexure RA/3 (Page** 436-440]

46. That the contents of para 52 of the Counter Affidavit are denied. It is submitted that so long as Respondent authorities are insisting on self-attested photocopies of Aadhaar card, it is only another identity proof and not any verifiable identity proof. In fact, in the large scheme of things, creation of database is the first commercial venture and making production of identity number mandatory for every single step will be the next commercial step so that the Government can generate sufficient income from the verification process thereby making UIDAI the most profitable venture. It is submitted that Aadhaar enrolment is a one time-one way process and there is no option available to a person to get his information deleted from the database. The so called choice is only limited to whether he/she wishes to himself link a bank account at the time of enrolment.

47. That the contents of para 53 of the Counter Affidavit are denied. The contents of para under reply has been dealt with above and are not repeated here for the sake of brevity.

48. That the contents of para 54 of the Counter Affidavit are denied. The contents of para under reply has been dealt with above and are not repeated here for the sake of brevity.

49. That the contents of para 55 of the Counter Affidavit are denied. The contents of para under reply has been dealt with above and are not repeated here for the sake of brevity.

The alleged attention of the Government to right to privacy of an individual as claimed is no more than a lip service.

REPLY TO DATA PROTECTION AND SECURITY

50. That the contents of para 56 of the Counter Affidavit are denied and it is stated that there is no framework for protection of data available in India and that position cannot be disputed.

51. That the contents of paras 57 and 58 of the Counter Affidavit are denied except in so far as it relates to matters of law. It is submitted that merely by criminalising a conduct, individual's data cannot be protected. The Petitioner further submits that the Information Technology Act, or guidelines framed there under are insufficient and adequet to afford protection under the UID scheme or to provide a justificaiton for the abridgments of rights under Articles 14 and 21. The IT Act specifically provides no protection against accidental loss of the data, destruction of the data or accidental disclosure of the data. Furthermore, one of the foremost questions raised in the petition is the regulation of third party processors who are engaged by the Respondents to process the data. The IT act provides no protection against the actions of such third parties since the disclosure policies of such companies are unknown and are also not controlled by any legislation. Wherever the power of misuse lies within the hands of the State itself, a specific regulatory mechanism is essential in a case such as the UIA scheme.

52. That the contents of para 59 of the Counter Affidavit are denied except in so far as it relates to matters of record. In

reply, it is submitted that the enrolment agencies are collecting personal information and data of private individuals upon whom UIDAI or Government of India does not have any real control apart from taking action for breach of contract and other usual actions of initiating criminal prosecution. The Petitioner has adverted to various instances of forgery committed by agents of enrolling agencies where FIR has also been lodged. However, the Respondents have not set out even a single instance of any action having been taken against any enrolling agency for dereliction and leakage of information and preparing fake or forged Aadhar cards. The Petitioner verily believes that the enrolling agencies work on a commission basis where they get paid for every enrolment done by them; leaving no incentive at all for them to either educate any persons on privacy or to be doubly sure of the credentials. The Petitioner further submits that the "strict control and supervision" claims made by the Respondent are only made in thin air, with no details available to the public about the same, let alone any concrete legislation or guidelines in this regard. It is submitted that the breach of terms and conditions of empanelment by enrolling agencies (by allowing fake identities to be generated) have not resulted in any convictions; but only termination of engagement. The extent of control by the government is negligible and nebulous to say the least.

53. That the contents of paras 60 to 65 of the Counter Affidavit are denied. It is denied that the security deployed for UID machinery/equipments is foolproof. Ultimately, these equipments are left with the hands of private enrolling

agencies and therefore the security cannot be guaranteed. It is submitted that UIDAI is not body corporate and is not capable of owning either the software or the database. The said software and the database naturally have to be vested in the President of India and the claim of ownership of UIDAI is therefore repelled. The Registrar General of India is an authority contemplated under the Census Act, 1948 and therefore to clothe him with the authority to maintain National Population Register under the Citizenship Act, 1948 with respect to information that is not contemplated under the Census Act, 1948 or the Rules framed thereunder is not permissible under the law. It is further submitted that the alleged UID scheme strategy to the extent it regulates individual's personal information requires to be legislatively authorised.

54. That the contents of paras 66 to 70 of the Counter Affidavit are denied. It is denied that the data security and privacy is of paramount concern for the Government, and had it been so, the Government would not have gone ahead with the UID scheme without first putting in place a privacy legislation to protect abuse of private and personal information.

55. That the contents of paras 71 and 72 of the Counter Affidavit are denied. The contents of paras under reply have been dealt with above and are not repeated here for the sake of brevity. The contents of paragraph under reply are misleading. It is submitted that the paras do not set out when the leakage of information is at the hands of somebody in control of the database as opposed to an attempt to hack the database. As alleged, even though instances of authentication can be made available to the individual

concerned, the individual concerned really has no control on the persons with whom the information is shared.

That the contents of paras 73, 74 and 75 of the Counter Affidavit are denied. It is submitted that it is evident that UID is permitting the State Governments to "leverage UID numbers for discharge of essential governmental functions" thereby making Aadhar virtually mandatory. The para under reply itself shows that UIDAI intends to share data. Further, the Respondents have also claimed that the Data that is collected is only stored in the Data Centres under the control of the UIDAI. However, as is evidenced from the Data Protection and Security Guidelines for Registrars, Paragraph 10 (3), the registrars can have data centres of their own for housing the data. These guidelines also fail to prescribe any liability, either penal or civil, that might be attached to the registrars in case of violations of the guidelines. Hence these guidelines remain declaratory in nature and are unenforceable.

REPLY TO THE GENESIS OF THE UNIQUE IDENTITY PROGRAMME

56. That the contents of para 76 of the Counter Affidavit are denied. As the para under reply is general in nature, it does not merit any specific reply.

57. That the contents of para 77 of the Counter Affidavit are not disputed.

58. That the contents of para 78 of the Counter Affidavit are denied as stated.

59. That the contents of para 79 of the Counter Affidavit are not disputed.

60. That the contents of para 80 of the Counter Affidavit are not disputed.

61. That the contents of para 81 of the Counter Affidavit are not disputed. It is however stated that the Process Committee's observation to create UIDAI by an executive order was without jurisdiction. The mandate of Process Committee was only in respect of unique identity for BPL families and not generally.

62. That the contents of para 82 of the Counter Affidavit are not disputed except in so far as it relates to matters of record. It is submitted that the notification dated 04.12.2006 is without jurisdiction in as much as when the Citizenship Act, 1955 does not contemplate a National Population Register, its merger with the Unique Identification Number project is not permissible. The Government has to function strictly in accordance with the statute and the Constitution.

63. That the contents of para 83 of the Counter Affidavit are not disputed except in so far as it relates to matters of record. It is submitted that any authority other than the President of India is capable of owning a property unless it is body corporate.

64. That the contents of para 84 of the Counter Affidavit are not disputed except in so far as it relates to matters of record. It is submitted that the objective which the UIDAI wanted to achieve could not have been done except under a statute.

65. That the contents of para 85 of the Counter Affidavit are not disputed except in so far as it relates to matters of record.

66. That the contents of para 86 of the Counter Affidavit are not disputed. It is however submitted that the UIDAI could not have been permitted except after a statute was passed by the Parliament.

67. That the contents of para 87 of the Counter Affidavit relate to matters of record and therefore need no reply.

68. That the contents of para 88 of the Counter Affidavit do not call for reply as they relate to matters of record. That in reply to the contents of para 88 of the Counter Affidavit it is submitted that the Planning Commission vide notification dated 28.01.2009 establishes an authority which is a subordinate organisation within and under the 'aegis' the Planning Commission and since it is not a juristic person, it can neither hold or own properties, nor can it enter into agreements/ contracts in its own right. It is submitted that creation of a body which is expected to "own" vital information about people of India and is likely to deal with interlinking of such information ought only to be done by means of a statute after due discussions in the Parliament. The executive power under Article 73 cannot be invoked for creation of body that collects private and personal data of Indian residents and stores them on a server.

69. That the contents of para 89 of the Counter Affidavit are not disputed. It is however submitted that the working of UIDAI is illegal and immoral.

70. That the contents of para 90 of the Counter Affidavit do not call for a reply from the Petitioner. It is submitted that a

Cabinet Committee, howsoever, eminent cannot replace the Parliament.

71. That the contents of para 91 of the Counter Affidavit are denied as stated. It is denied that any extensive study as alleged has ever been undertaken. In fact, any study as proposed ought to have been undertaken prior to launching of UID Scheme and creation of Respondent No.3 authority. From the records of the Writ Petition, it is clear that only after the enforcement of UID Scheme, a task force has been set up with a limited mandate to recommend the implementable solution for direct benefit transfer using Aadhar based authentic scheme and on any other topic as mentioned above. There is no study that seeks to test the efficacy of Aadhaar or UID scheme. The fact that no such extensive study was conducted prior to the implementation of the scheme is buttressed by the fact that a contract had already been entered into with a biometric service provider, L-1 Identity Solutions Operating Company Pvt. Ltd. On the 24th of August, 2010.

72. That the contents of para 92 of the Counter Affidavit are denied as stated. It is submitted that the objective of UID, i.e. to have a "universal" database of all the residents of India cannot be achieved until and unless the Government encroaches upon the fundamental and core private rights and therefore UIDAI is required to be statutorily provided. In so far as it is considered as a welfare initiative it does not provide a legitimate platform and can be a threat for every citizen of the country as it provides an unhindered share of private information.

REPLY TO THE BENEFITS PROVIDED BY UNIQUE IDENTITY SCHEME

73. That the contents of para 93 of the counter affidavit are denied as stated. It is submitted that there are several loopholes which were exposed by the sting operation conducted by the TV channels. However, UIDAI was unaware of the fraud and even after the TV sting exposed it, it did not file any FIR. The reported instances indicates that UID scheme is not completely transparent and a tamper proof system. There is no public interest in use of aadhaar by various government agencies. Aadhaar is only an additional identity proof and has been treated as such by the Government, and Enrolling Agents, who have always insisted on giving Aadhaar numbers to persons who have identity proofs. The perennial problem of identity proofs continues to persist for urban poor and migrant workforce, and Aadhaar does not solve any problems.

74. That the contents of para 94 of the counter affidavit are not disputed to the extent they relate to matters of record. Reference to previous attempts by the Government of India to provide identity-related documents has no bearing on the present facts. Previous attempts by various governments may also be illegal and unconstitutional, and the present aadhaar scheme could not be saved by reference to past efforts. It is the card for BPL families conceived vide approval dated 03.03.2006 that has metamorphosed into aadhaar scheme and thus reference to the same to justify aadhaar is scheme is plainly untenable. Attempts by Governments of

Andhra Pradesh and Karnataka are of no significance, as neither of them seem to have been preceded by any study and identification of real problem areas. There may be a vision in the 11th Plan Document, but certainly that vision cannot override the Constitution and the civil rights.

75. That the contents of para 95 of the counter affidavit are denied. It is submitted that the decision undertaken by the Empowered Group of Ministers and the Union Government is not appropriate for the reason that the Planning Commission is not a juristic person and therefore the ownership of a database cannot be vested in a non-juristic entity, which is not even accountable to the Parliament. Further, even though it is alleged that the issue of unique identifier had been deliberated at the highest levels of government for several years, but no such minutes of deliberation have ever been placed before this court. The so-called well considered decision of 2009 is also not accompanied by any (substantial) discussion on the issues raised in the present writ petition.

76. That the contents of para 96 of the counter affidavit are denied. It is submitted that though there is a need in the present scenario to have a "unique identifier" for all the citizens of the country but that can only be achieved if the same arises out of when it arises out of "authority of law". The executive power of the Union cannot in any manner overlap the legislative power of the Parliament. Further it is submitted that other identity cards for instance voter identity card is issued by Election Commission which is a statutory body framed under Constitution of India. Similarly, PAN card is issued by the Indian Tax Department under the supervision of the Central Board for Direct Taxes(CBDT),

which in turn draws authority from the Income Tax Act, 1961. Therefore no parity can be drawn between adhaar and other cards, which are being used for identity purposes. The problem of providing identity documents to the poor is not remedied by UID scheme.

77. That in reply to the contents of para 97 and 98 of the Counter Affidavit it is submitted that the objectives of the Aadhaar Scheme can only be achieved when they seek to have legal sanction, as the scheme make incursions on the fundamental rights of the people. Moreover it is submitted that National Identification Authority of India Bill, 2010 which was introduced in the Lok Sabha on 03.12.2010 itself signifies that the Respondents themselves are mindful that UIDAI requires a statutory basis. The e-Governance initiative of the Government in the areas of food security (PDS), jobs (MNREGA), health (Jsy), etc. through the UID Scheme can have serious repercussion like a single identity proof in the form of Aadhar no. can be very easily utilized for getting identity specifications of an individual. The leakage of one single number can cause irreparable injury/loss to an individual as that number is attached with various fields and accounts and in that circumstance the Government of India would not have any legal remedy for the same.

78. That the contents of para 99 of the Counter Affidavit are denied. It is submitted that the the technological advancements though necessary for the advancement of society but should not be a threat for the society. The agents and contractors that has been appointed by the Respondent No.3 have been so appointed without any due background check and as a consequence entities who have defrauded the

Governments have also been inducted as contractors like in Mysore the fraud of one of the enrolling agency by the name of COMPAT Technology was unearthed. Furthermore, it is submitted that in reply to the application moved under Right to Information to know the details of Contractors, Respondent No. 3 has itself informed the Petitioner that there is no way before it to ascertain the country of origin of the contractors.

79. The content of paragraph 100 of the counter affidavit is denied as stated except insofar as it relates to matters of record. It is submitted that the case cited in the paragraph in the reply were a different context and they do not even deal with the validity of the Aadhaar scheme. It is submitted that it does not appear from the judgements cited in paragraph under reply that it was brought to the attention of this honourable court that the Aadhaar rescued itself was under challenge before this court. Having not brought the set fact to the attention of this court, it is not open for the respondents to rely upon the said judgements insofar as it relates to production of identity proof.

REPLY TO THE SO CALLED 'ACHIEVEMENTS AND PERFORMANCE OF THE UID SCHEME 2009-2015

80. That the contents of para 101 of the Counter Affidavit are denied. It is submitted that though it said to be a volutanry scheme but in fact, soft methods have been deployed by Union and several State Governments making Aadhar requirement mandatory. For instance for getting subsidised LPG gas it is mandatory for a person to attach his Aadhaar Number with his bank account number, and inform the LPG

provider. Further, the same has also been mandatory for getting drivers license, arms license, vehicle registered etc.

81. That the contents of para 102 of the Counter Affidavit are denied. It is submitted that the social and economic wellbeing of the people cannot be achieved by UID Scheme, it seeks to provide only another identity card which has no real purpose. There is no material and pilot study to justify that the linkage of Aadhar number to other welfare schemes of the Government is going to bring any transformational changes, and such linkage is in any event contrary to the direction by this Hon'ble Court. UID Card can only link an existing bank account but cannot by itself provide payment to the workers and therefore it is not a social welfare scheme.

82. That the content of paragraph 103 of the counter affidavit are denied a stated. It is denied that the instant petition has been filed without considering the proper scope and width of the Aadhaar scheme. The UID scheme is indeed different from other schemes of the world, in that it on an unprecedented scale collects private information of the residents of a country and saves them in a remote server, without regard to any data protection or privacy laws. It is submitted that the Government is required to function within the framework of law and the Constitution and it cannot rely upon the ends to justify the means adopted.

83. That the contents of para 104 and 105 of the Counter Affidavit are not disputed except in so far as it relates to matters of record. It is denied that the UID scheme is implement in transparent, efficient, flexible and responsive

manner. The facts alleged to have been stated in respect of UID are denied as the deponent does not have any personal knowledge of the same, and puts the Respondents to strict proof thereof. However, it is stated that India is a republic limited by the Constitution, and therefore, mere (inflated and unverified) statistics cannot be the basis for legitimising a scheme which is otherwise an affront on the personal rights of the citizens and the residents of India.

84. That the contents of para 106 and 107 of the Counter Affidavit are denied as stated. It is stated that the source of statistics and data mentioned by the Respondent is not set out, and the statistics so cited is denied by the Petitioner. There is no theoretical correlation between LPG usage and Aadhaar except for the fact that making of aadhaar mandatory for LPG may have resulted in exclusion of certain persons, leads to increased black marketing as well. In response to three RTI's filed by the petitioner, being No. PLNG/RTI/5127 dated 23.10.2013, PLNG/RTI/5424 dated 06.12.2013 and PLNG/RTI/7705 dated 25.06.2015 seeking information regarding duplicate LPG connections from the IOCL, it was discovered that there were several instances of the same customer having duplicate connection when his Aadhaar number was linked with his LPG consumer number. The response very categorically stated that customers are not required to authenticate their identity at the time of delivery of cylinders, which appears contrary to the recommendations of the task force itself. The IOCL has also confirmed that they have done no analysis or investigation into the use of domestic LPG cylinders for commercial establishments and they have no estimate of the quantum of

use of subsidized LPG cylinders by commercial establishments. The statistical data provided by the Respondents is thus questionable, considering the vast number of fraudulent activities continuing in the case of LPG subsidies. True photocopy along with typed copy of the relevant portion of the Reply to RTI Application filed by the petitioner being No. PLNG/RTI/5127 dated 24..06.2015 is annexed herewith and marked as **Annexure – RA/4** (Page

True photocopy along with typed copy of the Reply to RTI Application filed by the petitioner being No. PLNG/RTI/5424 dated 06.12.2013 is annexed herewith and marked as **Annexure – RA/5** (Page

True photocopy along with typed copy of the Reply to RTI Application filed by the petitioner being No. PLNG/RTI/7705 dated 25.06.2015 is annexed herewith and marked as **Annexure – RA/6** (Page

Further, it is submitted that the recipient of the social welfare scheme cannot be put completely at the mercy of technology and those who control technology. UID Scheme cannot in itself provide a solution for the loss of LPG subsidies. It is submitted that UID Scheme cannot prevent a consumer from misusing the LPG Cylinder for a commercial purpose, after receiving subsidy in the bank. Hence, transferring subsidies in the bank does not serve the purpose.

85. That the contents of para 108 and 109 of the Counter Affidavit are denied as stated. In Mahatma Gandhi Rural Employment Guarantee Act (MNREGA), workers are paid their wages through a bank account or post office and as such the process of payment to the workers is by and large

unfair and improper, as it makes the villages, which are devoid of electricity and internet penetration dependent on technology. It is submitted that it is irrational and disproportionate to have UID project for the said purpose when the same objective is capable of being achieved by less intrusive and economical means. The limited problem of payment to MNREGA workers arises only due to insufficient reach of banks and post offices and the same cannot be overcome by provision of UID number. It is submitted that the focus of the government should to provide the means for the disbursement of the funds to those who are already registered, and tackling corruption. Only providing another identity is not a solution. The detailed table does not mention the criteria which the Government has undertaken to reach to those who are already registered but are not benefitted under the scheme. There are other processes like participatory planning and people's involvement in the program that needs to be leveraged and paid attention to.

86. That the contents of para 110 of the Counter Affidavit are denied as stated. It is submitted that it is a documented fact that India has a large part of population engaged in manual labour, which normally produces poorer biometric samples, leading to their exclusion, or higher chances of finger print mismatch. Linking of biometric attendance and payment through internet is another problem as the connectivity in interior parts is inadequate. Hence, all these factors do not stop rerouting of the wages of workers through middleman for which UID Scheme does not have any effective guidelines/measures.

87. That the contents of para 111 of Counter Affidavit are denied as stated. It is submitted that aadhaar itself is not capable of resulting in financial inclusion, as the banks continue to insist on "local address" despite the presence of address on aadhaar, which persists to be the roadblock in financial inclusion for migrant workforce.

REPLY TO THE SCOPE OF UID SCHEME WHEN COMPARED WITH THE UNIQUE IDENTITY SCHEME OF THE UNITED KINGDOM

88. That the contents of para 112 of the Counter Affidavit are wrong and denied except in so far as it relates to matters of record.

89. That the contents of para 113 of the Counter Affidavit are denied as stated. It is submitted that the reasons for having an identity card cannot be the basis for justification of the identity card/mechanism, so long as the mechanism is itself not permitted under the Constitution. In a press release by the London School of Economic's Department of Information System, titled 'An assessment of UK Identity Cards Bill and its implications: ID Cards-UK's high tech scheme is high risk', several possible risks associated with the ID scheme were highlighted. These risks were in no way related to the reason for having the identity card, but with the process of the same, which is nearly identical for the UID scheme. These risks, considering the quantum of information collected in India would be 10 times that collected in the UK, the risks and difficulties associated with the same also increase proportionately. Extensive literature in relation to the UK Identity Card establishes that the UK's endeavour was in

contravention of human rights and privacy laws applicable to it under the ECHR regime. It is submitted that the flavour of human rights under ECHR and that under the Indian Constitution is not very different. Thus, had the UK scheme been deployed for disbursement of social benefits it would have still been violative of the convention obligations. True photocopy along with typed copy of the relevant portion of the of a press-release by the London School of Economic Department of Information System, titled 'An assessment of UK Identity Cards Bill and its implications: ID Cards-UK's high tech scheme is high risk' dated 27.06.2005 is annexed herewith and marked as **Annexure- RA/7 (Page**

90. That the contents of para 114 of the Counter Affidavit are denied as stated. It is submitted that the UID Scheme is based on collecting personal data of an individual which is a direct infringement of the right of privacy guaranteed under the Indian Constitution and further the said data is stored in remote servers in a database form retrievable at a few clicks and can be conveniently shared. The implementation of any scheme by the government in no manner can encroach upon the fundamental right of a citizen. Furthermore it is submitted that there is widespread corruption in India; and there is no confidentiality/data protection of the data collected by Respondent No. 3, through private firms of questionable credentials, where a few of who have indulged in or facilitated criminal activities, some of which are under police investigation as well. The information collected under UID Scheme is valuable to criminals and for criminal activities and this makes the citizens vulnerable as well. The plea taken by the Respondent that under the Indian scheme:

(a) There are safeguards with respect to use of third party information is false.

(b) The data is shared after the person's consent, is no consent in the eyes of law. The scheme is a mandatory one. Especially, since all entries of NPR are to be seeded into aadhaar database and NPR is mandatory, it follows that aadhaar is also mandatory. Aadhaar and NPR are seeding information into each other, while the Government is put a façade that the scheme is not voluntary.

(c) There is no pooling of aadhar data with existing government databases is false.

(d) There is no function creep that is collection of race, religion and ethnicity data is false as relating silos of information makes such sharing possible. Further, "functional creep" is not only restricted to collection of information related to race, religion and ethnicity but the constant expansion of UID/Aadhaar as a pre requisite to availing benefits or services which are beyond or unrelated to the purpose for which it was brought to existence.

(e) Use is for limited purpose verification is false, as all authorities are insisting upon "aadhaar card" and everybody seems to be wanting a copy of aadhaar card, whether you wish to open a bank account, or even get a gate pass made in Government buildings.

That irrespective how many aadhaar numbers have been generated, the Government continues to be evasive on how many aadhaar cards have been printed and delivered to those persons in villages and in interior hinterland of country.

91. That the contents of para 115 of the Counter Affidavit are denied. It is submitted that there is no end-to-end transparency effected by impugned scheme. The UID/Aadhar Scheme does not stand the test of reasonableness and rationally accountable functioning of the executive, which is the essence of democratic governance. Hence, it is submitted that the Government has not effectively used UID for de-duplication. Furthermore, it is submitted that there is no provision for the residents to opt out from the UID project and information once given cannot be deleted or destroyed at the instance of the applicant-resident. It is not as if a person not willing to receive any "benefits" from the Government can decide not to enrol for the scheme.

92. That the contents of para 116 and 117 of the Counter Affidavit are denied as stated. It is submitted that the biometrics does not enhance the value of Aadhaar card rather it creates a false sense of security. It is submitted that the arguments regarding the "biometric" being *found* suitable is an illusionary argument as no tests and study was conducted prior to the launch of aadhaar scheme by the erstwhile Government, which is being faithfully implemented by the present Government as well. Furthermore, the contention of the Respondents that the collection of Biometric Data is fool proof is itself misplaced. In a paper titled *Biometric Identification: Device Specification ad Actual Performance Considered for the Operations of the UIDIA,* authored by Hans Varghese Mathews, it is concluded that the biometric data collected is not free from errors. It is also denied that the relying on foreign perspectives has no relevance. It is submitted that reliance must be placed on

tried and tested methods abroad where a novel scheme is brought to the country, especially since our country has no proper data protection or privacy legislation in place. For instance, in South Africa, the Director General of home affair's duty to implement the national identification system and population register essentially entails consideration of citizen's privacy in the information that is collected. Further, the Human Rights Commission not only has the authority to pursue violations of privacy and human dignity, but also has the responsibility to monitor infringements of divergent concerns such as access to courts, political rights, education, and social security. Besides these protections the constitution of South Africa itself explicitly recognizes a right to data privacy. In pursuance of this The Protection of Personal Information Act, 2013 was enacted in order to promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith. It is submitted that reliance on such schemes in countries like South Africa is pertinent especially in the light of similarity of the objects and nature of the scheme, and complete dissimilarity or lack of any protections guidelines or legislations relating to

security and protection. True photocopy along with typed copy of the relevant portion of the paper titled 'Biometric Identification: Device Specification ad Actual Performance' Considered for the Operations of the UIDIA, authored by Hans Varghese Mathews published in December 2012 is annexed herewith and marked as **Annexure – RA/8** (Page

93. That the contents of para 118 of the Counter Affidavit are denied as stated. It is submitted that the example of USA is wrongly cited, and there also there no UID scheme like the one in India. Reference to USA and EU countries cannot be made unless they are accompanied by comparison of the applicable regime with prevailing in India. It is submitted that in addition to collection of biometric, it is (A) sharing of data; (B) linking of data; and (C) storage of data remotely that are of concern, which factors may be absent in various countries to which abstract reference has been made in the paragraph under reply. The cost of aadhaar scheme does not justify the end it seeks to achieve, which is eventually paid by the taxpayers like the Petitioner.

REPLY TO THE SCOPE OF ABUSE OF THE UID SCHEME

94. That the contents of para 119 of the Counter Affidavit are denied as stated. An aadhaar card system will lead to a slippery slope of surveillance and monitoring of citizens, and in fact already, aadhaar which was introduced initially for BPL identification, has now been made mandatory in property transactions and income tax returns, making surveillance easy – which is not contemplated under the Constitution that seeks to guarantee rule of law. It is not the possibility of

abuse, but actual abuse which is the reasons for striking it down. Reliance at this juncture is made to doctrine of abuse of rights, which seeks to limit the ability of the invoker of a right or obligation, i.e. the Government in the present case.

REPLY TO THE ALLEGATION THAT THE WRIT PETITION IS BASED ON ACADEMIC GROUNDS ETC

95. That the contents of para 120, 121 and 123 of the Counter Affidavit are denied as stated. It is submitted that the grounds taken by the petitioner are not hypothetical and are supported by valid proof and documents. The concerns and issues raised by the Petitioner are genuine issues that implore for adjudication, as the said issues have never arisen before this Hon'ble Court and have arisen purely on account of high handedness of the Government in innovating and implementing the aadhaar scheme. The queries made by the Petitioner through the RTIs in various government departments gave an analysis of the extent of field study incorporated by the authorities while implementing the entire scheme.

96. That the contents of para 122 and 123 of the Counter Affidavit are denied as stated. It is submitted that views taken by individuals and thinkers as well as constitutional experts cannot be taken lightly and ignored. Indian democracy is proud of its traditions of having consultative governments, the views taken by the experts cannot be brushed aside. The wisdom of the Government has not only been questioned by various scholars but has also been questioned by the Parliamentary Standing Committee, whose

successive reports have only been ignored by the Government, which is absolutely arbitrary and unfair. It is submitted that proceeding by way of notification issued under authorisation of Council of Ministers when the legislation is pending is contrary to principle of constitutional morality. The Constitutional contemplates limited governance and seeking of accountability, inter alia, through parliamentary – legislative process. Thus, it is violative of the fabric of the Parliamentary process interwoven into the Constitution to do indirectly what cannot be done directly. Furthermore, each of the ministers forming the Council of Ministers are part of the elected representatives in the Parliament, and thus, when the Parliament is seized of the matter, it is improper and impermissible for its members to snatch the issue away from the Parliament and take a decision, or to take steps that render the Parliamentary process nugatory.

REPLY TO PARAWISE REPLY

97. That the contents of para 1 of the Counter Affidavit are denied as stated and in response the contents of para 1 of the Writ Petition are reiterated to be true and correct. It is denied that UID is a well-considered scheme, or it is based only on apprehensions. The instant it petition is a public interest litigation which seeks to rates substantial questions of law. It is submitted that petitioner had moved to Regular First Appeal before the Karnataka High Court as the suit filed by the petitioner had been dismissed under Order VII of CPC, to which order, principles of res judicata not apply.

Furthermore the Appeal has been dismissed as withdrawn and is therefore no longer pending.

98. The contents of paragraph 1A of the counter affidavit are denied as stated and it is submitted that it has not been disputed even by the respondents that an appropriate representation had been preferred by the petitioner before the Prime Minister. It is only been disputed that the petitioner has elected a wrong forum in writing and representation to the Prime Minister. The contents of paragraph 1A of the writ petition are reiterated to be true and correct.

99. The contents of paragraph 2 of the counter affidavit are denied as stated, and in response contents of paragraph 2 of the writ petition filed reiterated to be true and correct. It is reiterated that information in respect of origin of the bidding companies is being deliberately hidden and not being provided to the petitioner. It is has been stated by the Respondents in the para under reply that the CIPO was not required to "research" into the origin of and control of any foreign company and provide such details as had been sought by the petitioner. It is submitted in this light that it is evident from a bare reading of the contract of UIDAI with M/s L1 identity Solutions Operating Company blatantly shows that the country of origin is the United States of America. The first page of the contract itself discloses that L1 is a subsidiary of a US Company by the name of Delware. The acceptance letter dated 16th July 2010 of L1's bidder commercial quote which is found at annexure L to the contract contains the US address of the company as well. Therefore it is submitted that the statement of the

respondent that available details has been provided by the UIDAI is false and it is reiterated that this act of the Respondent goes to show that the information sought is being deliberately hidden.

a. The contents of paragraph 2(a) do not call for any response.
b. The content of paragraph 2(b) of the Counter Affidavit are baseless, misconceived and denied as stated. It is submitted that the petitioner is well within its rights to approach the Delhi High Court in respect of denial of information under the Right to Information Act. However the filing of the said it petition does not take away the obligation of the respondents to provide all necessary details to the Petitioner as sought by his application under the Right to Information Act.
c. That the contents of paragraph 2 c) of the counter affidavit are denied and in response contents of paragraph 2 c) of the writ petition are reiterated to be true and correct.
d. That, the contents of paragraph 2 of the counter affidavit do not call for reply.
e. That the contents of paragraph 2 e) of the counter affidavit are denied as stated and in response content of paragraph 2 e) of the writ petition is a reiterated to be true and correct. It is submitted that all necessary facts have been discloses in the writ petition and there is no suppression of fact as alleged or otherwise.

100. That the contents of paragraph 3 of the counter affidavit are denied as stated and it is submitted that the impleadment

application in the contempt petition and the present writ petition are on different footings. Therefore merely because an impleadment application was filed it does not follow that the petitioner cannot file of full-fledged writ petition before this honourable court. It is denied that the writ petition has been disposed of; and it is submitted that what has been disposed of his only an interlocutory application in the contempt petition.

101. The contents of paragraph 4 of the counter affidavit are denied as stated and in response contents of paragraph 4 of the writ petition are reiterated to be true and correct. Despite there being various reporting of fake Aadhaar card being generated, no action has been taken by respondent no. 3 against any person. It goes to show that these reports are not being taken seriously by the respondents. It is submitted that the statistics been relied upon by the respondents not disclose the source from which it is based and as such they are denied. Further the petitioner has no means of ascertaining the veracity of these statistics which anyway cannot give the validity to the scheme which has to be a justified only on the parameters provided in the Constitution. The cost of rolling out the project is disproportionately high as compared to savings that it seeks to project and therefore is not justifiable at all. It is submitted that if the success of the other scheme is to be justified by the savings that it has made in respect of distribution of welfare services and a transfer of money etc. to the citizens, then there is no reason to make other compulsory high-value property transactions as well as in filing of income tax returns. It is also denied that savings are

accrued due to the UID scheme using the "data" given in the three tables at page 83 of the Counter. It has not been explained by the Respondents whether the "duplicated detected" was using the Aadhaar/UID, or otherwise. Further, the resulting "savings" demonstrated by multiplying the number of duplicates by the respective welfare amounts is denied. If the "duplicates" were detected by seeding the existing databases of these welfare programs, then to establish savings it will require to be shown that the subsidies were being withdrawn against the so called duplicates detected, which will then further require to be investigated as to who received the stolen subsidies.

102. That the contents of paragraph 5 of the counter affidavit are denied as stated and in response contents of paragraph 5 of the writ petition are reiterated to be true and correct. It is a reiterated specifically that NPR is a compulsory mechanism which has been most intelligently clubbed with so called "voluntary &consensual scheme" – Aadhaar, thereby making Aadhaar also mandatory scheme. It is denied that NPR and Aadhaar have separate database.

103. That the contents of paragraph 6 of the counter affidavit are denied as being evasive and incorrectly stated.

(i) That the contents of paragraph 6(i) are denied as stated, except in so far as it relates to matters of record.

(ii) That the contents of paragraph 6(ii) are denied as stated, except in so far as it relates to matters of

record. The Petitioners reserves his right to reply to the para under reply during the course of oral arguments.

(iii) That the contents of paragraph 6(iii) are denied as stated, except in so far as it relates to matters of record.

(iv) That the contents of paragraph 6(iv) does not call for a response from the petitioner.

(v) That the contents of paragraph 6(v) are denied as stated, except in so far as it relates to matters of record.

(vi) That the contents of paragraph 6(vi) are denied as stated, except in so far as it relates to matters of record. It is submitted that Aadhaar is a massive project, which has been initiated without conducting any study on the utility and efficacy, accuracy of using biometrics and retina as identity markers. Eventhough it was launched with limited objectives, it it has now started to spread its tentacles in various forms seeking to first get seeded in silos of information and then to link the said silos of information, exposing private information. A situation cannot be continence that the Aadhaar number of the entire army is on a database, and all the personal details of army officers are available to any person on a single click.

(vii) That the contents of paragraph 6(vii) are denied as stated, except in so far as it relates to matters of

record. It is submitted that the so-called significant differences between the UK ID card project and UID scheme are not significant differences at all and in fact it will appear that the Indian project is far more daemonic in character. Even though the sole purpose of UID scheme is allegedly to facilitate access to service and benefits for the residents form of governmental and non-governmental sector, it introduces great security risk by collecting individual's data and keeping it on a server. It is also apparent from the paragraph under reply that what started as a seat of services and benefits from the government has now also expanded to include services from "non-governmental sector" - which means that the government is capable of making various private services including private medical care, purchase of services, purchase of vehicles, are linked to Aadhaar scheme. It is submitted that already even if one opens a private bank account Aadhaar card is being demanded by the bank authorities, implying clearly that other has been roped in by the government for all private sector activities as well –where none was warranted. The respondents have not stated as to which so-called "expert body" has considered the issue of national ID cards and in what manner, and therefore any apply in this regard is it best weak, evasive and liable to be rejected.

(viii) That the contents of paragraph 6(viii) are denied as stated, except in so far as it relates to matters of record. It is a matter of record that person when enrolled into NPR is automatically enrolled into

Aadhaar, and vice versa. This aspect has been dealt with by affidavits filed in the other connected matters and therefore is not being expanded hereupon for the sake of brevity. Further, in an RTI reply No. TC UID/Admin/RTI06/Vol XII/2014-2015, the Respondents have admitted that over 191 million people who enrolled in NPR were issued UID/Aadhaar numbers. It is submitted that the Citizenship Rules are also *ultra vires* section 14 A of the Citizenship Act 1955 and also *ultra vires* the Constitution of India, and therefore reliance thereupon by the respondent is of no help.UIDAI provides the software for BEL the sub-registrar of RGI and the scanners used by BEL are as specified by UIDAI. These ensure that every enrolment data is sent to UIDAI and a UID / Aadhaar number is automatically issued to the person enrolling in NPR. True photocopy along with typed copy of RTI reply dated 13.11.2014 with Ref No. TC UID/Admin/RTI06/Vol XII/2014-2015 is annexed herewith and marked as **Annexure – RA/9**(Page

(ix) That the contents of paragraph 6(ix) are denied as stated, except in so far as it relates to matters of record. The petitioner reserves the right to deal with the arguments raised in this paragraph at the time of hearing at it relates only to matters of law. It is submitted that would the citizenship act contemplates is merely a register a citizen's whereas Aadhaar is not a register of citizens, but a register of residents.

(x) That the contents of paragraph 6(x) are denied as stated, except in so far as it relates to matters of record. In response thereto contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xi) That the contents of paragraph 6(xi) are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xii) That the contents of paragraph 6(xii) of the Counter Affidavit do not call for a reply.

(xiii) That the contents of paragraph 6(xiii) of the Counter Affidavit do not call for a reply.

(xiv) That the contents of paragraph 6(xiv) of the Counter Affidavit do not call for a reply.

(xv) That the contents of paragraph 6(xv) are denied as stated, except in so far as it relates to matters of record. In respondents contents of para under reply of the Writ Petition are reiterated to be true and correct. Accenture Services P Ltd (New Delhi) is a subsidiary of the tainted Accenture LLP which is been prosecuted for corruption and payment of kickbacks and this being the case, where there are serious doubts about integrity of a group company a subsidiary of the same company cannot be allowed to collect private data of Indian residents. The fact that Accenture India was engaged

in the past by the Respondent does not make the fact of engagement of a doubtful entity by the Government of India any less culpable.

(xvi) That the contents of paragraph 6(xvi) of the Counter Affidavit do not call for a reply.

(xvii) That the contents of paragraph 6(xvii) of the Counter Affidavit do not call for a reply.

(xviii) That the contents of paragraph 6(xviii) of the Counter Affidavit are denied as stated. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xix) That the contents of paragraph 6(xix) of the Counter Affidavit do not call for a reply.

(xx) That the contents of paragraph 6(xx) are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that making aadhaar based identity verification for use by private sector and holding a competition to develop mobile applications based on aadhaar platform are all endeavours of and geared towards economic model of aadhaar. It is submitted that levy of fees, where none should have been levied is indeed a commercial enterprise. Firstly, aadhaar is not required as an identity model for over 97% percent cases (given that only 3% enrolments

have been done without reference to any other existing ID documents). Secondly, one the hand the Government claims to provide "identity" to those who do not have it and then is charging fees for such provision, which is otherwise essential state function is indeed a commercial venture. It is submitted that being "State" under the social contract, the State is under an obligation to provide the said "service" without any charge from any one. It is submitted that private sectors deploying aadhaar based verification services indeed have to pay verification fees, which is further passed on to consumer (in a noticeable form or otherwise). It is submitted that the a database is not owned by the Government of India and where Respondent No.3 has been projected as a separate body – in such a situation, the fees is not likely to be deposited in the Consolidated Fund of India. In any event, deposition of such profit and fees in the Consolidated Fund of India does not take away the undercurrent of commercial venture well thought out by Sri Nandan Nilekani, the then in charge of the venture.

(xxi) That the contents of paragraph 6(xxi to xxiv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is reiterated that enrolling agencies and registrars have found ways and means to make enrolment for aadhaar 'mandatory' as a matter of fact. It is submitted that the so called 'sine

quo non' consent of individuals is meaningless if by softer methods aadhaar is made mandatory. Furthermore, if the so called consent is voluntarily given then the Respondent No.3 should also withdrawal from aadhaar scheme, in that a person should be permitted to delete his data by a simple application to authority. It is submitted that aadhaar number is only an *additional* identity proof for those who have already identity cards and as such enrolment on the basis of introducers or letters of MPs/MLA's etc. is negligible, about which the Respondents have not disclosed any data.

(xxii) That the contents of paragraph 6(xxv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xxiii) That the contents of paragraph 6(xxvi) of the Counter Affidavit do not call for any reply from the Petitioner.

(xxiv) That the contents of paragraph 6(xxvi) are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is denied that the para (xxvi) of the Writ Petition is speculative in character.

(xxv) That the contents of paragraph 6(xxvii) and 6 (xxviii) are denied as stated, except in so far as it relates to

matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that there is no detail of any action taken by UIDAI that has been enumerated in the para under reply in respect of COMAT Technologies.

It is pertinent to point out herein that in response to an RTI filed by the petitioner, bearing no. A-11018/01/13/RTI-Vol.-V/UIDI/Lucknow/1332 (HI), it was discovered that action is being taken against fraud or violation of procedural guidelines based on an Office Memorandum issued by the UIDAI, being OM No. 4(4)/57/249/2014-E&U. As per the said OM, the only penalties that have been prescribed are blacklisting, suspension or of persons guilty of fraudulent activities. However, no criminal proceedings have been initiated against any such persons as per the RTI reply. Thus, the Respondent's claim that appropriate penal action is being taken remains unsubstantiated and rebutted. The Respondent has also heavily relied on the IT act to put forth that Criminal proceedings could be initiated against persons involved in fraud or data theft. However, there is no evidence of any such action being taken, despite there being several instances of malpractices in RTI enrolment as admitted by the Respondents. This furthers the petitioner's contention that unless an appropriate legislation is present providing adequate safeguards, the process of issuance of UID cards can never be transparent and secure. It is also submitted that no further details of any action taken by the UIDAI against any other agency has been

provided in the Counter Affidavit, and hence, the reply is at best evasive.

Further it is denied as stated by the respondent that entering into a contract with L1 identity solutions highlights the vendor neutrality approach adopted by the UIDAI.It is reiterated that that entering into such contracts poses great threat to national security and privacy of individuals. Clause 14 of the contract entered into by the UIDAI which contains the Ownership and Retention policy goes to show that documents are to be retained with the company for a period of seven whole years. Clause 15 further goes to show that Identity Solutions may have access to personal information of the Purchaser and/or a third party or any resident of India. Annexure B to the contract enables biometric service providers, in this case L1 to collect transfer store or otherwise process information that pertains to specific individuals and can be linked to them. These clauses goes to show that there is a tremendous amount of private data that is vulnarable to misuse by biometric service providers like L1. Further in view that L1 is a subsidiary of a US company, the possibility that US Surveillance laws mandate disclosures of data leaves the sensitive data in the hands of these service providers such as L1 vulnerable to access by other countries like the US and thereby poses a threat to security as well.

(xxvi) That the contents of paragraph 6(xxix) are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under

reply of the Writ Petition are reiterated to be true and correct. It is submitted that there is no prior study that he been done, and there exists no material to justify the launch of aadhaar scheme. Task force was set up after launch of the aadhaar scheme, and the mandate of the task force was justify and explain how to deploy aadhaar; and it was not the mandate of the said task force to re-examine and validate the aadhaar scheme itself. As stated in the Writ Petition, this is the only force/committee that was constituted in relation to examination of aadhaar and its usefulness, and whose mandate for pre-fixed. The Petitioner relies on the contents of para 113 of the Counter Affidavit for this purpose.

(xxvii) That the contents of paragraph 6(xxx) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is reiterated that given the strong objections made by the Standing Committee itself, the rolling out of aadhaar scheme is highly improper.

(xxviii) That the contents of paragraph 6(xxxi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The decision of AIR 1958 Kerala 290 is distinguishable on facts and further

the law laid down there is not the proposition of law applicable to the facts of the present case.

(xxix) That the contents of paragraph 6(xxxii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. In the para under reply, in the Counter Affidavit, the Respondent No.3 has not set out as to what background checks are performed by them, and as such an adverse inference ought to be drawn in this respect. The para under reply is a clear case where UIDAI is attempting to arrogate its responsibility arising out of empanelment of doubtful agencies to the Government of Karnataka. It is submitted it is this very evasion of responsibility and accountability that buttress the case for a statutory for regulation of collection of personal information. It is submitted that despite that fact that CAG Report which had material in respect of COMAT Technologies was for year ending 31.03.2011, the very same entity was again empanelled for the year 2011-2012. It is denied that UIDAI had no mechanism to verify the credentials of a bidder who applies for empanelment, and in fact for UIDAI to say that "*there is no way UIDAI would have had this knowledge at the time of empanelment of M/s COMAT Technologies*" goes to establish the level of care shown by UIDAI in the matter of national security. It has also come to the Petitioner's knowledge that COMAT has since been taken over by some other company. Having no proper guidelines or policy in

place, questions relating to such scenarios in order to maintain complete protection of data are left in the air.

(xxx) That the contents of paragraph 6(xxxii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of para under reply are hyper technical in nature, and aims to defeat the ends of justice.

(xxxi) That the contents of paragraph 6(xxxiii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xxxii) That the contents of paragraph 6(xxxiv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xxxiii) That the contents of paragraph 6(xxxv and xxxvi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The Petitioner fails to understand as to what could be reservation of the present Government to first enact a statute and if and as permitted by the Parliament the

scheme could be rolled out. It is submitted that the protection that UIDAI seems to give to the database could well be entrenched in a statute.

(xxxiv) That the contents of paragraph 6(xxxvii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that in previous paragraph full details have been given about action of State of Karnataka, however, Respondent No.3 is pleading ignorance in case of State of Maharashtra. The response is paragraph under reply is certainly more than meets the eyes.

(xxxv) That the contents of paragraph 6(xxxviii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xxxvi) That the contents of paragraph 6(xxxix) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that the Petitioner has made all the due disclosures in law.

(xxxvii) That the contents of paragraph 6(xl) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto,

contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that in consultative democracy like India, it is not a constitutional tradition of this country to ignore and brush aside the reports of the Standing Committee, which have been prepared by consultative mechanisms by Senior Parliamentarians. The issues raised in the report are extremely germane especially those relating to national security. It is denied that the present regime is sufficient to deals with the collection, storage and disclosure and use of sensitive personal data of individuals.

(xxxviii) That the contents of paragraph 6(xli) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The Petitioner has learnt that the position on the ground is different from what is stated in the Counter Affidavit. Further directing the Ministries to follow a payment gateway/framework where aadhaar is mandatory itself is goes to show how the orders passed by this Hon'ble Court are being ignored. It is submitted that "encouragement" to the DBT beneficiaries to enrol for aadhaar is more a matter of compulsion than option or volition.

(xxxix) That the contents of paragraph 6(xlii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are

reiterated to be true and correct. It is reiterated that aadhaar does not solve the problems related to LPG distribution, which is more a problem of error in inclusion and exclusion, and corruption. It is submitted that the previous de-duplication processes were not carried out diligently, and were perhaps marred by corruption. It is denied that aadhaar is superior method of verification.

(xl) That the contents of paragraph 6(xliii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that the averments in para under reply, i.e. where aadhaar has been issued less than one year ago it needs to be accompanied by another proof of address go to show that aadhaar is actually a waste of public resources money, because it is unable to be CONCLUSIVE proof of residence of a person.

(xli) That the contents of paragraph 6(xliv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(xlii) That the contents of paragraph 6(xlv) of the Counter Affidavit does not call for any response.

(xliii) That the contents of paragraph 6(xlvi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. Other allegations are dealt with in the preceding paragraphs and are not repeated herein for the sake of brevity. It is false to say that UOD scheme is less intrusive for availing services. It is submitted that in a system that is rampant with corruption and payment of "commission" in securing payments, aadhaar does not secure solution on a continued basis. Despite aadhaar and DBT, for continued payments necessary 'convenience' charges will have to be still paid by the recipient for processing of payment etc., and hence, tackling of corruption is the most basic of all requirements. UID based attendance system has its own limitations, which are not at all considered by the Respondents. It is submitted that reference to ends to justify the means is impermissible and therefore UID cannot be justified by reference to the means. In any event, UID scheme is not itself the "correct criteria" and to project itself as a welfare scheme is misleading. It is but one of the tools. It is also denied that the Pradhan Mantri Jan Yojana does not mandate use of the UID scheme because of the voluntary nature of the scheme. The reason for the same is the Supreme Court order directing that no person should suffer for want of the Adhaar card.

(xliv) That the contents of paragraph 6(xlvii) of the Counter Affidavit are denied as stated, except in so far as it

relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xlv) That the contents of paragraph 6(xlviii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xlvi) That the contents of paragraph 6(xlix) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that it is not open to the Respondent to hide behind the shield of "policy decision" for matters that are to be essentially provided for by legislation and which involves expenditures of huge amounts of public monies. It is submitted that almost at all the places, whether in banks or in other places (such as mobile phone connection), what is required is a proof of local address and therefore a "portable" aadhaar with so called national-roaming of identity is a complete farce. The petitioner is not aware and cannot confirm the

veracity of the contents of the report "The World Food Programme" and its comment on the alleged utility of UID scheme.

(xlvii) That the contents of paragraph 6(l) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is reiterated that due to interlinking of silos of information, it is possible to find various sets of information about an individual from aadhaar itself.

(xlviii) That the contents of paragraph 6(li) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xlix) That the contents of paragraph 6(lii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. The Petitioner fails to understand the theoretical

relationship between aadhaar and falling consumption in LPG. It can only be explained by 'exclusion' on account of DBT.

(l) That the contents of paragraph 6(lii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. However, it is submitted that the process explained the para under reply supports the case of the Petitioner, that without verification cylinder is being delivered. Hence, it allows corruption at the level of delivery man and distribution agencies.

(li) That the contents of paragraph 6(liv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that the fact is that order dated 23.09.2014 has not been modified and continues to be binding. However, the Respondent No.3 is violating the order dated 23.09.2014 and all that it seems to have done is to file an application for clarification / modification, a copy of which has not even been served on the Petitioner. The allegations on the conduct of the Petitioner are denied as being vexatious and false. It is submitted that the Petitioner is well within its rights to raise all questions

in the present exhaustive Writ Petition which can all be adjudicated at the time of final hearing.

(lii) That the contents of paragraph 6(lv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is denied that the Government has taken privacy issues seriously and in fact, is proceeding to ignore the right to privacy and storing personal data of persons, forcefully, on their servers. There is no option to delete that data available with the persons who have enrolled for aadhaar. It is submitted that the grounds taken for not producing the bid documents under the RTI is not the same as is pleaded in the Counter Affidavit and further, parts of the said documents have been made available to the Petitioner. In any event, the said documents could be presented to the court in a sealed envelope, and if the court decides that the document ought not to be disclosed it is a separate matter. The alleged confidentiality and sensitivity does not save the documents from being judicially considered and be the basis for an action of judicial review. It is denied that there is any suppression of material facts by the Petitioner. It is submitted that the guidelines for PIL does not limit the scope of power under Article 32, and they simply cannot.

(liii) That the contents of paragraph 6(lvi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(liv) That the contents of paragraph 6(lvii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lv) That the contents of paragraph 6(lvii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lvi) That the contents of paragraph 6(lix) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lvii) That the contents of paragraph 6(lx) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lviii) That the contents of paragraph 6(lxi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is stated that aadhaar is only projected as a voluntary scheme, but is actually not a voluntary scheme. In fact, as per the Respondents own case , for transfer for DBT in LPG, biometric validation of aadhaar number is not done. This clearly implies that even a dead person can continue to receive benefits under DBT. There is no opt-out mechanism available, and failure to authenticate would only mean that authentication is failed and not that a person has opted out of the aadhaar system.

(lix) That the contents of paragraph 6(lxii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of

paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lx) That the contents of paragraph 6(lxiii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxi) That the contents of paragraph 6(lxiv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxii) That the contents of paragraph 6(lxv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. There is no reason at all for having NDEC category, and passing on the subsidy to such organisation.

(lxiii) That the contents of paragraph 6(lxvi) of the Counter Affidavit are denied as stated, except in so far as it

relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. The slogan of 'Minimum Government, Maximum Governance' is akin to promoting surveillance, where by presence of methods of surveillance – curbing people's privacy, 'governance' is achieved.

(lxiv) That the contents of paragraph 6(lxvii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is reiterated that only a very small number of enrollments have been done through the introducer system, making aadhaar only an alternative form of identity document which is based on existing identity related documents such as PAN Card, Drivers License, Voter ID card etc. As per data produced by the Respondent No.3 only 2,13,800 enrolments have been done through introducer system, which is a very small number. Further, 'Introducer' system has resulted into introduction of improper persons, some of whom are illegal migrants. Also, it is not as if the existing aadhaar card holders can introduce a person, but only a certain designated person can be introducer – and this makes the whole process chimerical.

(lxv) That the contents of paragraph 6(lxviii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxvi) That the contents of paragraph 6(lxix) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that given the federal polity that India is, there has never been and there actually is not, a need for having a single identity card valid across the country. In any event, identity proofs issued by the State Governments have been recognized across the country and likewise for proofs issued by the Central Government. Thus, a disproportionate measure impinging upon right to privacy could not have been embarked by the Respondents. It is submitted that there is not a single person cited as example by the Respondent, which felt deprived as he was not covered by an existing 'card' regime.

(lxvii) That the contents of paragraph 6(lxx) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto,

contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is denied that the para of the Writ Petition under reply is based on conjectures. It is denied that sharing of residents follows any due process as alleged or otherwise. It is submitted that "due process" cannot be what is decided by Respondent No.3 without regard to any statute and without any powers having been delegated to it.

(lxviii) That the contents of paragraph 6(lxxi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that the law as it stands today only permits NoRIC and does not permit NPR, and hence to establish and setup NPR is illegal and unconstitutional. Information from NPR is being shared with UID and vice versa, and therefore, if one enrols in NPR, his/her details are automatically entered into aadhaar database.

(lxix) That the contents of paragraph 6(lxxi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are

reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that the process adopted for collection of data for NPR (not NORIC) is not provided in the statute and could not therefore be done.

(lxx) That the contents of paragraph 6(lxxii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxxi) That the contents of paragraph 6(lxxiv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxxii) That the contents of paragraph 6(lxxv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that the manner in which 'consent' is being

obtained by UIDAI has rendered 'consent' as no consent in the eyes of law. Consent is taken at the time of enrolment, where no one briefs any individual about the consent and ramifications of the so called consent given by him or her.

(lxxiii) That the contents of paragraph 6(lxxvi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that yet again details of action taken have not been specified, and it is not clear as to how such enrolling agencies are held accountable or whether they are held accountable at all.

(lxxiv) That the contents of paragraph 6(lxxvii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that once the card/number has been issued, the purpose for which the UID scheme is floated pales into insignificance. It is submitted that all the studies setout in the para under reply are oriented towards one outcome – justify the aadhaar scheme and expenditure related thereto. Therefore, it follows that these studies

are only a study of ends but not of the means, and hence they do not fulfil the test of proportionality.

(lxxv) That the contents of paragraph 6(lxxix) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that the so called confidentiality is big façade because it rests on 'consent' of individual, and such 'consent' has been taken without disclosing full information and consequences.

(lxxvi) That the contents of paragraph 6(lxiv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxxvii) That the contents of paragraph 6(lxxx) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that UIDAI organised HACKATHON in

January 2015 to develop applications based on aadhaar platform, and there is an evident economic motive behind aadhaar scheme. Introduction of aadhaar enabled biometric attendance system is violative of the order dated 23.09.2012 by which this Hon'ble Court has been pleased to direct that no person should suffer for want of aadhaar. It meant that the Government could not make aadhaar compulsory in any quarter.

(lxxviii) That the contents of paragraph 6(lxxxi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxxix) That the contents of paragraph 6(lxxxii) of the Counter Affidavit are denied as stated. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(lxxx) That the contents of paragraph 6(lxxxiii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. It is submitted that comparisons with other countries have to be made keeping in mind the information that the card/scheme seeks to collect and store (and how), and not by the purpose of the card. It is submitted that what is

common to all the countries, i.e. UK and USA is that scheme was floated under a statute, whereas there is no statute in India in this respect. Further, the purpose of the scheme is usually shunned once the scheme is implemented. Hence, while the avowed objective of aadhaar is to ensure transfer for benefits from the Govt to an individual, it is now being used as a simple identity proof for various transactions such as opening bank accounts, obtaining mobile connections, obtaining LPG connection (even without subsidy) etc. Thus, from the current trends it is evident that the original purpose of aadhaar is lost.

(lxxxi) That the contents of paragraph 6(lxxxv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. That the contents of paragraph 6(lxxxi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is submitted that the judgments in Sharda v. Dharampal and Bhabhani Prasad Jena cited by the Respondents do not further the case of the Respondents. Further, the case (2011) 113 BOM LR 3107 is also not applicable to

the facts of the case. It is denied that the submission of information by the resident is because "*resident opts to provide for obtaining social welfare benefits..*" It is submitted that many persons who have enrolled for aadhaar had to do so because aadhaar number was required for availing one or other government services such as property rights registration, marriage registration, obtaining drivers license etc.

(lxxxii) That the contents of paragraph 6(lxxxvi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct.

(lxxxiii) That the contents of paragraph 6(lxxxvii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. Aadhar, when connects silos of information is capable of generating all knowledge about residents.

(lxxxiv) That the contents of paragraph 6(lxxxviii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of

paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxxxv) That the contents of paragraph 6(lxxxix) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. The "confirmation" paragraph by which consent is provided on a pre printed form (at page 194 of the Counter Affidavit) yet again proves the Petitioners point. It is submitted that there is no bifurcation between enrolment process and sharing of information and the consent is common. Therefore, with a person there is no choice whether he wishes to only enrol and does not wish information to be shared. The enrolment is therefore on "take it, or leave it" basis.

(lxxxvi) That the contents of paragraph 6(xc) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity. It is impermissible for the Government to go ahead with UIDAI scheme, when NIDAI Bill is pending and has yet not been passed by the Parliament.

(lxxxvii) That the contents of paragraph 6(xcii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxxxviii) That the contents of paragraph 6(xciii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(lxxxix) That the contents of paragraph 6(xciv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xc) That the contents of paragraph 6(xcv) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xci) That the contents of paragraph 6(xcvi) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xcii) That the contents of paragraph 6(xcvii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xciii) That the contents of paragraph 6(xcviii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xciv) That the contents of paragraph 6(xcix) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xcv) That the contents of paragraph 6(c) of the Counter Affidavit are denied as stated. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xcvi) That the contents of paragraph 6(ci) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xcvii) That the contents of paragraph 6(cii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xcviii) That the contents of paragraph 6(ciii) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

(xcix) That the contents of paragraph 6(civ) of the Counter Affidavit are denied as stated, except in so far as it relates to matters of record. In response thereto, contents of para under reply of the Writ Petition are reiterated to be true and correct. The contents of paragraph under reply are repetitive in nature and are not again dealt with here for the sake of brevity.

104. That the contents of para 7 of the Counter Affidavit are formal in nature and need no reply.

105. That the contents of para 8 of the Counter Affidavit are denied as stated. It is asserted that the Petitioner has cause of action and good reasons to approach this Hon'ble Court.

REPLY TO PARAWISE REPLY TO THE GROUNDS

106. The petitioner reiterates the grounds taken in the Writ Petition and nothing not specifically dealt with in this Counter Affidavit may not be deemed as admitted merely for non traverse.

A-D The Petitioner reiterates the contents of grounds A-D. It is denied that UID scheme is capable of being covered within the scope of Art 73 of the Constitution and no law is required for the same, given the scope of UID scheme.

E The Petitioner reiterates the contents of ground E. It is denied that aadhaar is in fact a voluntary scheme. It is denied that aadhaar is in line with Directive Principles Of State Policy.

F. The Petitioner reiterates the contents of ground F. It is submitted that non consideration of the successive reports of

the Standing Committee of the Parliament is contrary to Constitutionalism and consultative traditions of Indian democracy. It is denied that the concerns of the Standing Committee have been addressed by Respondent No.3.

G. The Petitioner reiterates the contents of ground G.

H The Petitioner reiterates the contents of ground H. The suggestion that prerogative of the Government to allocate the work/department at the place where is it is most suited is absolute in nature and is not regulated by the Principles of Constitutionalism.

I. The Petitioner reiterates the contents of ground I.

J The Petitioner reiterates the contents of ground J. It is submitted that the necessary backgrounds checks have not been undertaken and had it been undertaken the Respondent No.3 would have found out about M/s COMAT Technologies. It has also not been rebutted by the Respondent, that eventually, India and Pakistan both have the same service provider for provision of technology to generate identity cards.

K. The Petitioner reiterates the contents of ground K. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

L. The Petitioner reiterates the contents of ground L. It is reiterated that when silos of information are connected together, it will be possible to integrate all data concerning an individual, which possibility cannot be ruled out.

M. The Petitioner reiterates the contents of ground M. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

N. The Petitioner reiterates the contents of ground N. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above. It is denied that there is any consultation with "all stakeholders" as alleged.

O. The Petitioner reiterates the contents of ground O. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above. It is denied that there is any "real option" with the residents given accessing essential governmental interactions have been made conditional upon procuring aadhaar number. There is no opt out clause and in law there is no reason to not have opt out clause. Failure to authenticate by a resident would result in disentitlement.

P. The Petitioner reiterates the contents of ground P. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

Q. The Petitioner reiterates the contents of ground Q. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above. It is denied that individuals who have enrolled have given their free and fair consent, or that the consent is informed consent. This aspect has been dealt with above and is not repeated herein for the sake of brevity. It is stated that while UID is pitched entirely on providing proof of identity to those who do not have any identity related documents, but about 97% enrolments are those who have existing identity related documents.

R. The Petitioner reiterates the contents of ground R. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

S The Petitioner reiterates the contents of ground S. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

T The Petitioner reiterates the contents of ground T. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

U&V The Petitioner reiterates the contents of grounds U & V. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

W The Petitioner reiterates the contents of ground W. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above.

X The Petitioner reiterates the contents of ground X. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above. It is denied that UID scheme is a well thought out scheme.

Y. The Petitioner reiterates the contents of ground Y. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above. It is submitted that UID/Respondent No.3 contemplates unabashed sharing of data between Government departments, without fresh intimation to the person concerned. Thus, the UID scheme is actually a scheme for surveillance, though labelled as a welfare scheme.

Z The Petitioner reiterates the contents of ground Z. The reply by the Respondent to the ground is repetitive in nature and has been dealt with above. It is submitted that the financial aspects even of a socio economic development project ought to be taken into account and the same cannot be launched without knowing the financial implications. India is a country with limited means and strict financial choices are to be made, and therefore the country cannot afford to spend money in areas where none is required.

107. That before concluding here it is respectfully stated that even private sector companies are seeding Aadhaar numbers for their employees, even though no delivery of "welfare services" is being performed by them. This manifests the idea of possibility of the use of Aadhaar for surveillance in future. True photocopy along with typed Copy of the Advertisement dated 13.01.2014 of Trident Group published in the Newspaper 'Economic Times' is annexed herewith and marked as **Annexure – RA/10 (**Page_____

108. That, for the facts and reasons as aforestated, it is submitted that the instant Writ Petition be allowed with costs.

109. No new facts or material not already in the Writ Petition have been taken in the instant affidavit.

110. That the Annexures mentioned in the accompanying Rejoinder Affidavit are true typed copies of their respective originals.

111. That the contents of the above Rejoinder Affidavit are true and correct to best of my knowledge and belief, no part of it is false and no material has been concealed therefrom.

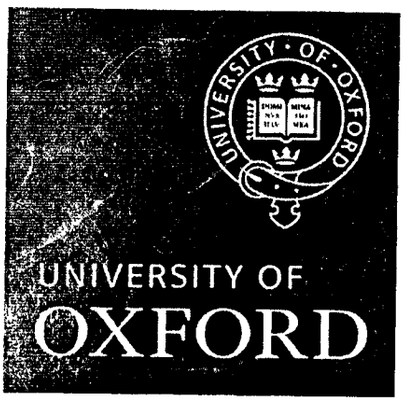
DEPONENT

VERIFICATION:

Verified at New Delhi on this_____day of_____, 2015 that the contents of our aforesaid Affidavit are true and correct to the best of my knowledge and belief, no part of it is false and no material has been concealed therefrom.

DEPONENT

Annexure RA-1 101



Oxford Pro Bono Publico
http://www.law.ox.ac.uk/opbp

BIOMETRIC IDENTIFICATION AND PRIVACY

Comparative research prepared for the Centre for Law and Policy Research, India

February 2013

102

CONTRIBUTORS

Faculty:

Dr David Erdos
Katzenbach Research Fellow &
Leverhulme Trust Early Career Fellow

Research coordinators:

Chintan Chandrachud
OPBP Treasurer
MPhil Candidate

Chris McConnachie
OPBP Chairperson
DPhil Candidate

Tamas Szigeti
OPBP Events and Liaison Officer
MPhil Candidate

Researchers:

Lauren Dancer
BCL Candidate

Julian Ensbey
BCL Candidate

Natasha Holcroft-Emmess
BCL Candidate

Anjoli Maheswaran Foster
BCL Candidate

Ram Mashru
MSc in Contemporary India Candidate

Angela Pavao
MSt in Criminology Candidate

Sarah Tulip
BCL Candidate

Mark Zarwi
BCL Candidate

The research coordinators would like to thank:

- **Professor Timothy Endicott**, Dean of the Oxford Law Faculty, for his support of this project,
- The Members of the Oxford Pro Bono Publico Executive Committee, **Professor Sandra Fredman, Dr Tarunabh Khaitan, Mr Miles Jackson, Ingrid Cloete, Emma Webber,** and **Richmond Glasgow**, for their support and assistance with the project.

Indemnity

Oxford Pro Bono Publico (OPBP) is a programme run by the Law Faculty of the University of Oxford, an exempt charity (and a public authority for the purpose of the Freedom of Information Act). The programme does not itself provide legal advice, represent clients or litigate in courts or tribunals. The University accepts no responsibility or liability for the work which its members carry out in this context The onus is on those in receipt of the programme's assistance or submissions to establish the accuracy and relevance of whatever they receive from the programme; and they will indemnify the University against all losses, costs, claims, demands and liabilities which may arise out of or in consequence of the work done by the University and its members.

Intellectual property

104

TABLE OF CONTENTS

PART A **1**

SUMMARY OF RESEARCH **2**

Introduction 2

Background 3

Biometric Information and the Right to Privacy 4

The Justification of Interferences with Privacy Rights 6

Safeguards for the Protection of Biometric Data 8

PART B **13**

UNITED STATES **14**

Overview 14

Legal Framework 15

Case Law 17

ISRAEL **21**

Overview 21

Legal Framework 21

Case Law 23

AUSTRALIA **26**

Overview 26

Legal Framework 26

Case Law and Political Debate 28

COUNCIL OF EUROPE **30**

Overview 30

Legal Framework 30

Case Law 32

EUROPEAN UNION **36**

Overview 36

Legal Framework 36

Case Law and Political Debates 38

UNITED KINGDOM **41**

Overview 41

Legal Framework 41

Case law and Political Debate 43

FRANCE **46**

Overview 46
Legal Framework 46
Case Law 47
GERMANY 50
Overview 50
Legal Framework 51
Case Law 52

PART A

SUMMARY OF RESEARCH

INTRODUCTION

1 This report has been prepared to assist the Centre for Law and Policy Research in drafting a petition to the Supreme Court of India, challenging the constitutional validity of the Unique Identification Number (UID) scheme, otherwise known as the 'Aadhaar' scheme.

2 The UID scheme aims to issue all 1.2 billion Indian residents with a universal identification number, linked with biometric and demographic data that will be stored on a centralised database. Three types of biometric data will be collected: facial photographs, finger prints and iris scans.[1] If completed, this will be world's largest biometric database. However, India currently lacks comprehensive data privacy protection laws and the draft National Identification Authority of India Bill 2010 contains limited safeguards.[2]

3. OPBP has been requested to prepare research on two questions:

   a. Have biometric identification schemes in other countries been challenged on privacy grounds?

   b In jurisdictions that collect biometric data, what measures are in place to protect citizens' right to privacy?

4. Our research covers eight jurisdictions, selected because they use biometric identification schemes and based on the expertise of our researchers. These are the United States of America (US), Israel, Australia, the Council of Europe, the European Union (EU), the United Kingdom (UK), France, and Germany.

5. This report consists of two parts. This part, Part A, provides a summary of our research, drawing out key points that are relevant to the petition challenging the UID scheme. Part B provides information on the specific jurisdictions, dividing the discussion of each jurisdiction into three sections: an overview of the jurisdiction,

[1] For the purposes of this report, biometric data is defined as data relating to an individual's physiological and behavioural characteristics, allowing for individual identification or verification See EU Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 'Working Paper 80. Working document on biometrics' (2003) 12168/02/EN, 2

[2] See Graham Greenleaf, 'India's national ID system: Danger grows in privacy vacuum' (2010) 26 Computer Law & Security Review 479, 480 and 487

the relevant legal framework, and the relevant case law on biometric identification schemes. Where there is no case law, we have considered the political debates over these schemes. We hope that Part B will be useful should the Centre for Law and Policy Research wish to explore the issues discussed in this summary in greater detail.

6. This summary covers four topics:

   a. Background;

   b. Biometric information and the right to privacy;

   c. The justification of interferences with privacy rights;

   d. Safeguards for the protection of biometric data.

BACKGROUND

7 In the US, Israel, France, and Germany, the right to privacy is constitutionally and legislatively protected. In these jurisdictions, either the written constitutions have expressly enumerated the right to privacy or one of their provisions has been interpreted as including this right. The European Convention on Human Rights (applicable in the Council of Europe Member States) and the European Charter on Fundamental Rights and Freedoms (applicable in the EU) expressly contain a right to privacy. In Australia and the UK,[3] although the right to privacy is not constitutionally protected, it is protected by primary legislation.

8. All of the jurisdictions in our study have data protection laws which apply to personal data. In the European context, 'personal data' is defined as 'any information relating to an identified or identifiable individual'.[4] Biometric data is considered to be a class of personal data and is therefore subject to protection.[5] A similar approach has been adopted in the US,[6] Israel,[7] and Australia.[8]

---

[3] The UK does not have a written constitution, in the sense of a codified document

[4] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data European Treaty Series No 108, adopted 28 Jan 1981 (Council of Europe Convention), art 2(a) (Data Protection Convention); EU Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, art 2(1) (EU Directive).

[5] See EU Working Party, 'Working Paper' (n 1) section 3.1. See further *S and Marper v UK* (2009) 48 EHRR 50 discussed at para 10 below

[5] Council Directive 95/46/EC (n 4) art 8(1).

[6] See United States, para 35 below

See Israel, para 56 below.

[8] See Australia, para 66 below.

9. Biometric identification schemes are in operation in all of the jurisdictions considered in this study. The purposes of these schemes are diverse and include the prevention of crime,[9] immigration control,[10] identity protection[11] and the maintenance of security standards for passports.[12]

BIOMETRIC INFORMATION AND THE RIGHT TO PRIVACY

10. In the European context, the collection of personal data in databases by the state, including the collection of biometric data, is generally considered to be an interference with the right to privacy, requiring justification.[13]

11 In *S and Marper v United Kingdom*[14] the European Court of Human Rights (ECtHR) held that:

> [T]he mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.[15]

The applicants were arrested and charged with criminal offences in the UK. One of the applicants was acquitted and the case against the other was discontinued. Deciding on whether it was permissible for the UK police to retain fingerprints, cellular samples and DNA samples collected from the applicants, the Grand Chamber of the ECtHR observed that these data fell within the realm of 'personal data' and the retention and storage of these data was an interference with the applicants' Article 8(1) right to a private life under the European Convention on Human Rights (ECHR).[16] The Court ultimately found that this interference was disproportionate.[17]

---

[9] See discussions on the US (paras 27-30 below) and France (paras 118-120 below).
[10] See US, para 28
[11] See Israel (para 52 below), France (para 115 below), UK (para 106 below).
[12] See in particular EU, para 93-94
[13] The European Court of Human Rights appeared to affirm this position in *Marper* (see n 14 below), but its Art 8 jurisprudence under the European Convention on Human Rights is not yet settled.
[14] *S and Marper v UK* (2009) 48 EHRR 50.
[15] ibid [121].
[16] ibid [121].
[17] ibid [125] Discussed further below at para 23

12. The German Federal Constitutional Court adopted a similar approach in the *Census Act Case*.[18] This case involved a challenge to the National Census Act 1983, which placed an obligation on every household to fill in and return a census form for the collection of statistical data. There the Court held that the protection of 'informational self-determination' fell within the ambit of the 'right to the free development of one's personality' under article 2(1) of the German Constitution

> Individual self-determination, however, presupposes – even under the conditions of modern information processing techniques – that the individual has the freedom to decide whether to perform or omit actions, including the possibility of acting according to this decision. A person who cannot safely tell what information about him regarding certain areas is known to his social environment, and cannot to some extent assess the knowledge of potential partners of communication, can be essentially inhibited in his freedom to make autonomous plans and decisions. ... *It follows that the free development of one's personality under the modern conditions of data processing presupposes the protection of the individual against unlimited collection, storage, use and transmission of his personal data.*[19]

13. In a 2012 decision, the French Constitutional Court, the *Conseil Constitutionnel*, affirmed a similar principle in striking down portions of a law authorising the implementation of a national biometric identification scheme and the creation of a national biometric database.[20] The *Conseil* held that biometric data constitute 'personal data' and that the right to respect for private life under the French Constitution requires that:

> [T]he collection, registration, conservation, consultation and communication of personal data must be justified on grounds of general interest and implemented in an adequate manner, proportionate to this objective.[21]

14. The US Supreme Court has also confirmed that the right to privacy under the US Constitution includes 'an individual interest in avoiding disclosure of personal

---

[18] BVerfG 15 December 1983, *BVerfGE* 65, 1, 43 – *Census Act Case ('Volkszahlung')*, discussed in S Michalowski and L Woods, *German constitutional law: the protection of civil liberties* (Ashgate 1999) 120-123

[19] ibid 42-43 (emphasis added).

[20] Décision n° 2012-652 DC du 22 mars 2012 (Official English translation available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil-constitutionnel-105428.pdf> accessed 21 February 2013)

[21] ibid [8].

matters'.[22] However, the US is distinct from the European jurisdictions in that it does not engage in a two-stage balancing exercise. Instead, justificatory considerations are built into the enquiry whether the right to privacy has been violated, with the result that mere collection, storage, or disclosure of personal data are not considered to be automatic violations of this right.[23]

THE JUSTIFICATION OF INTERFERENCES WITH PRIVACY RIGHTS

15. The jurisdictions considered in this report apply different tests in ascertaining whether the restrictions imposed on the right to privacy are justified. Courts in the EU and the Council of Europe apply a three-part test requiring that limitations must: (a) be in accordance with the law; (b) serve a legitimate aim; and (c) be 'necessary in a democratic society'.[24] The last requirement involves a proportionality analysis, requiring the Court to determine whether the limitation is suitable for achieving its aim (suitability), whether there are less restrictive means to achieve this aim (necessity), and whether the extent of the limitation is outweighed by the achievement of the aim (proportionality in the 'narrow sense').[25]

16. In the US, a softer standard of review has been applied in privacy cases, with courts largely focussing on the rationality of legislative restrictions on the right to privacy.[26] However, the degree of deference accorded by courts to the legislature and the executive has often depended upon the nature of the information sought to be collected. In *Whalen v Roe*,[27] a statute that required physicians to report details of patients to whom they had prescribed certain drugs was challenged on privacy grounds. Although the US Supreme Court concluded that the statute did not constitute a violation of the right to privacy, Justice Brennan observed that '[t]he central storage and easy accessibility of computerized data vastly increase[d] the potential for abuse of that information' and that future developments might compel

[22] *Whalen v Roe*, 429 US 589, 97 S Ct 869, 51 L Ed 2d 64, Stevens J at 599. The Supreme Court has held that privacy interests are protected under the 1st, 4th and 14th Amendments of the Constitution. See *Katz v United States*, 389 U.S. 347 (1967), *Griswold v Connetiicut*, 381 US 479, 85 S. Ct. 1678 and *Stanley v Georgia*, 394 U.S. 557 (1969).

[23] See US, para 41ff below.

[24] See Council of Europe, paras 73-74, EU, para 87

[25] See Aharon Barak, *Proportionality: Constitutional Rights and Their Limits* (CUP 2012) chs 9-12.

[26] See *Whalen v Roe* (n 22) 597. See also *Thom v New York Stock Exchange*, 306 F Supp 1002 (1969) 1011; *Iacobucci v City of Newport, Ky*, 785 F 2d 1354 (1986) 1355.

[27] ibid

'some curb on such technology'.[28] Further, courts have looked upon databases storing 'sensitive information' (as the term is understood in the US) with a more critical eye. In *US v Westinghouse*,[29] the Court of Appeals for the Third Circuit declined a challenge to a subpoena granted to a health and safety inspector mandating an employer to disclose its employees' medical records. The Court held that the constitutional right to privacy had not been breached, since the information contained in the medical records was not 'sensitive'.[30] It laid down a number of factors that should be considered in deciding whether an individual's right to privacy was violated, including 'the type of record...the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated'.[31] The point was put clearly by the Court of Appeals for the Ninth Circuit in *Doe v Attorney General*: 'the more sensitive the information, the stronger the state's interest must be'.[32]

17. The US understanding of 'sensitive information' should be contrasted with the definition of 'sensitive data' in other jurisdictions. In Europe and jurisdictions inspired by the European data protection model, sensitive data is defined as personal data revealing certain protected characteristics, including 'racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [and]... relating to criminal convictions'.[33] Some, but not necessarily all, types of biometric data may be classified as sensitive information. The EU Working Party on the Protection of Individuals with Regard to the Processing of Personal Data suggests that facial images in particular should be regarded as sensitive data as they have the potential to reveal ethnic or racial origin.[34] Sensitive data is subject to heightened safeguards and may not be automatically processed except in defined circumstances. In Australia, the Privacy

[28] ibid 607.
[29] 638 F 2d 570
[30] ibid 579.
[31] ibid 578
[32] 941 F2d 780
[33] See Data Protection Convention (n 4) art 6; EU Directive (n 4) art 8
[34] Working Party, 'Working document on biometrics' (n 1) 10. The Working Party is comprised of representatives from data protection authorities in all EU Member States, the European Data Protection Supervisor, and a representative of the EU Commission. See Council Directive 95/46/EC (n 4), art 29.

Act 1998 was recently amended to include all biometric data as 'sensitive information', which must be managed with particular care.[35]

18 Other types of data that have resulted in courts being less deferential include data with personal references (which are not anonymised or statistically prepared)[36] and personal data that have undergone automatic processing.[37]

SAFEGUARDS FOR THE PROTECTION OF BIOMETRIC DATA

a) Legal safeguards

19. Given that the collection, processing and storage of biometric data are generally considered to be interferences with the right to privacy, adequate legal safeguards are required for these interferences to be justified. In General Comment 16 on the article 17 right to privacy in the International Covenant on Civil and Political Rights, the Human Rights Committee emphasised that:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorises or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[38]

Similarly, in *Marper*, the ECtHR stressed that:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private... life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent

---

[35] The amendment was made by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, Schedule 1, s 42

[36] *Census Act Case* (n 18)

[37] *S and Marper v UK* (n 14) [103]

[38] UNHRC 'General Comment 16. The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art 17)' (1988) [10] <http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument> accessed 21 February 2013

> any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the 'protection of personal data undergoing automatic processing is concerned ... The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse ....[39]

b) Common features of safeguards

20. The countries in this study have adopted very similar legal safeguards governing the collection, use and storage of personal data, including biometric data. These safeguards are framed and applied in somewhat different ways, but they share at least nine common features:[40]

a **Purpose specification**: Data must be collected for specified, explicit and legitimate purposes.

b. **Data quality:** Data collected should be relevant and necessary to accomplish the legitimate purposes for which it is being collected.

c. **Data collection:** Data should be given with the consent or knowledge of the data subjects.

d. **Notice:** Data subjects should be informed about the purposes for which the data are being collected, the authority authorising data collection, whether disclosure is mandatory or voluntary, and the consequences of non-provision, among other matters.

e. **Limitations on use:** The data should only be used for the purposes originally specified, or purposes compatible with those purposes. Restrictions also apply to the transfer of data between state organs and between the state and private organisations or individuals.

f **Security:** Appropriate security measures should be in place to ensure the security, integrity and confidentiality of personal data.

g. **Access:** Data subjects should have a right to access their personal data held in databases.

---

[39] *S and Marper v UK* (n 14) [103].

[40] What follows is adapted from Graham Greenleaf's ten 'universal' elements of global privacy law, outlined in Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 International Data Privacy Law 68, 73

h. **Correction:** Data subjects should have the right to update and correct this data.

i. **Independent data protection authority:** All jurisdictions in this study also provide for an independent data protection authority to monitor compliance with data privacy safeguards and to investigate and act on complaints.

21 As noted above, European and European-inspired jurisdictions also require heightened safeguards for 'sensitive data', relating to certain protected characteristics.[41]

c) Challenges to biometric identification schemes

22. Our research has identified three recent cases involving challenges to biometric identification schemes: the ECtHR's decision in *S and Marper v United Kingdom*,[42] the petition against Israel's biometric identification scheme in *Nahon v Knesset*,[43] and the French *Conseil Constitutionnel* decision on the national biometric identity card scheme.[44] In these cases, the existence and adequacy of legal safeguards were central to the courts' assessment of whether these interferences with the right to privacy were justified.

i) S and Marper v United Kingdom

23 As introduced above, in *Marper* the applicants argued that the UK police's retention of their fingerprints, cellular samples and DNA profiles after charges against them were dropped was inconsistent with the right to respect for private life enshrined in Article 8 ECHR. In assessing whether this interference was proportionate, the Court placed weight on the fact that the UK was the only Member State of the Council of Europe which permitted indefinite retention of fingerprint and DNA data [45] It compared the practice of the majority of other Member States, which required such samples to be removed or destroyed either immediately or within a certain time after acquittal or discharge.[46] The blanket and indiscriminate nature of its powers of retention meant that the UK had overstepped its margin of

[41] Above para 17.
[42] Above n 14
[43] HCJ 1516/12 *Nahon v. Knesset* S.CT 842 (2012) (judgment available in Hebrew) <http://elyon1.court.gov.il/files/12/160/015/c03/12015160.c03.htm> accessed 21 February 2013.
[44] Above n 20.
[45] ibid [110]
[46] ibid [108]

appreciation and failed to strike a fair balance between the competing public and private interests. Accordingly, the retention of the applicants' data was a disproportionate interference with their right to respect for private life and a constituted a violation of Article 8 ECHR.[47]

24. The Grand Chamber's approach in *Marper* therefore indicates that a national system of collection and retention of biometric information must incorporate sufficient safeguards in order adequately to protect the right to respect for private life under the ECHR. It appears that by 'appropriate safeguards', the Court means that the law must include requirements against indefinite storage.[48]

ii) Nahon v Knesset

25 The necessity of collecting biometric data in a centralised database was debated in the Israeli High Court of Justice in *Nahon v Knesset*.[49] The petitioners challenged the Israeli Law for Including Biometric Identifying Means and Data in Documents of Identification and in Databases 2009 and a proposed two-year pilot programme to test biometric identification. The legislation provides for the embedding of biometric data (fingerprints and computerized tags of facial features) in Israeli identification cards and passports, and allows for the creation of a database containing biometric data on all Israeli citizens.[50] The petitioners specifically challenged the creation of a central database of biometric identification, arguing that this was not necessary to achieve the purpose of accurately identifying Israeli citizens.[51] It was argued that it was possible to embed biometric data on smart ID cards and to check identity against these cards, without creating a centralised database. The Court ultimately dismissed the petition as premature, given that the pilot programme had not yet been completed. However, at the hearing the Justices strongly criticised the scheme, demanding that the Interior Ministry rework its planned pilot programme to evaluate whether it is actually *necessary* to store the population's biometric data in a single, centralized database. In the wake of the

[47] ibid [125]
[48] For further discussion of this case see Council of Europe, para 78 below.
[49] Above n 43
[50] Rawlson King, 'Israeli jurists right to call biometric database "extreme" and "harmful"' *BiometricUpdate.com* (30 July 2012) <www.biometricupdate.com/201207/israeli-jurists-right-to-call-biometric-database-extreme-and-harmful/> accessed 21 February 2013
[51] The Association for Civil Rights in Israel, 'Introduction from ACRI Petition to the High Court of Justice. Objections to a Governmental Biometric Database' (February 2012) <http://www.acri.org.il/en/wp-content/uploads/2012/02/biometric.pdf> accessed 21 February 2013.

2006 theft and dissemination of Israel's Population Registry, containing data on nine million Israeli citizens, the Justices were particularly concerned that a centralised biometric database would bring greater security risks.[52] Since the hearing, the Interior Ministry has been exploring other options,[53] as well as evaluating safeguards to prevent data leaks and information theft.[54]

iii) Conseil Constitutionnel decision

26. In 2012, the French Constitutional Court, the *Conseil Constitutionnel* (*Conseil*), struck down portions of legislation which introduced a national identity card containing biometric information (face image and fingerprints), and provided for the creation of a national database for this data.[55] The court found that the Act served the legitimate aim of preventing identity fraud. However, the *Conseil* found that the legislation exceeded this legitimate purpose by authorising the police and other law enforcement agencies to access the database for purposes unrelated to the prevention of fraud.[56] Therefore, the *Conseil* found that this was a disproportionate restriction of the right to privacy.[57] It should be noted, however, that the *Conseil* did not take issue with the creation of a population-wide biometric database per se.[58]

---

[52] See Israeli Ministry of Justice, 'Theft and Online Dissemination of Israel's Population Registry' <http://www.justice.gov.il/MOJEng/ILITA/News/crackedcase.htm> accessed 21 February 2013.

[53] ibid

[54] For further discussion of this case see Israel, para 58 below

[55] Above n 20

[56] ibid [10]. 'that the technical characteristics of this database as defined by the contested provisions enable it to be consulted for purposes that other than the verification of an individual's identity' (Official English translation)

[57] ibid [3]

[58] For further discussion of this case see France, para 115 below.

PART B

UNITED STATES

OVERVIEW

27. Federal agencies have authority to collect personally-identifiable information. The principal federal biometric schemes in the US are the Integrated Automated Fingerprint System (IAFIS) and the Automatic Biometric Identification System (IDENT). Databases at the federal and state level are 'interoperational' and integrated.[59]

a) IAFIS

28. The IAFIS is a FBI-maintained automated fingerprint identification and criminal history database. It contains a range of information: fingerprints; criminal histories; mug shots; physical characteristics such as height, weight and hair and eye colour; and aliases. The IAFIS also includes the fingerprints of current and former US military personnel and federal government employees. It is currently the largest biometric database in the world.[60]

b) IDENT

29. The IDENT is a system for storing and processing biometric, limited biographic and encounter-related information, administered by the Department of Homeland Security.[61] It includes the US-VISIT program, which collates biometric data from non-citizens seeking entry. Originally developed for immigration control purposes, the system is now used for 'national security, law enforcement, immigration, intelligence and other DHS mission-related functions.'[62]

---

[59] The FBI, Department for Homeland Security (DHS) and Department of Defence's biometric databases are interoperable allowing free exchange of data. State level databases are integrated with those at the federal level in so far as all fingerprint and DNA data is shared with the FBI directly, and in certain limited instances with the DHS.

[60] See generally FBI, 'Integrated Automated Fingerprint Identification System', <http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis> accessed 21 February 2013.

[61] The data stored include, but are not limited to fingerprints, photographs, name, date of birth, nationality, and other personal descriptive data and the context of the interaction with an individual including but not limited to location, document numbers, and/or reason information collected. See generally DHS, 'Privacy Impact Assessment for the Automated Biometric Identification System', <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf> accessed 21 February 2013.

[62] Department for Homeland Security, 'Privacy Impact Assessment for the Automatic Biometric Identification System (IDENT), 31 July 2006 (an overview of the IDENT system is provided at 2-4).

c) Other

30 In addition, each state has its own biometric database and a DNA database.[63] Fingerprinting is pervasive and is required by numerous state and federal laws across a range of non-criminal contexts, such as federal securities law[64] and laws concerning employment in bartending[65] and day-care.[66]

LEGAL FRAMEWORK

a) Overview

31 The Supreme Court has held that privacy interests are protected under the 1st, 4th and 14th Amendments of the Constitution.[67] States have also recognised a qualified right to privacy, expressly or impliedly.[68]

32. The US is considered to be an outlier among developed countries, as it does not have comprehensive data privacy legislation applying to both the public and private sector.[69]

33. At the federal level, the key piece of legislation is the Privacy Act 1974,[70] a federal statute placing general safeguards on information processed and held by the federal government.[71] This is supplemented by Guidance[72] and Privacy Impact Assessments.[73]

34. A huge number of additional federal and state statutes relate to individual privacy rights in discrete areas.

[63] J Lynch, 'From Fingerprints to DNA: Biometric Data Collection in US Immigrant Communities and Beyond' (Immigration Policy Centre 2012) 6 < https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond> accessed 21 February 2013

[64] 15 USC § 78q(f)(2) (2006).

[65] *See Iacobucci v City of Newport*, 785 F2d 1354 (6th Cir 1986) (a city ordinance requiring employees at places where liquor is served to be fingerprinted by the police was not unconstitutional, discussed further below).

[66] See California Health and Safety Code § 1596.871(a), (b)(1)(A)-(D), (c)(1) (2006).

[67] See *Katz v United States*, 389 U.S. 347 (1967), *Griswold v Conneticut*, 381 US 479, 85 S. Ct. 1678 and *Stanley v Georgia*, 394 U S 557 (1969).

[68] <http://www.ncsl.org/default.aspx?tabid=13467> explaining that constitutions in 10 states expressly recognise the right to privacy, while the highest courts of other states have established constitutional privacy rights.

[69] See Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 International Data Privacy Law 68, 70.

[70] 5 USC § 552a (2006).

[71] It applies only to data processing by the federal government and not to state governments or to the private sector

[72] Department of Defence Privacy Program, DoD 5400.11-R, May 2007

[73] Above n 63

121

b) Safeguards under the Privacy Act 1974

35. The Act requires federal agencies, as data collectors, to adopt minimum standards for the collection, use, maintenance and dissemination of personal records.[74] However, the statute has been criticised for failing to provide sufficiently robust protection, particularly in relation to biometrics.[75] The establishment of a separate commission to ensure oversight of the Privacy Act was resisted. The act thus fell under the purview of the Office of Management and Budget and implementation has been deemed unsatisfactory.[76] The Act's main requirements are explained below.

i) No disclosure without consent (subject to significant exceptions)

36. Federal agencies are prohibited from disclosing any record, 'except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.'[77] However, this general rule is subject to 12 enumerated exceptions.[78]

ii) Individual right of information and access

37. The data subject must be informed of: the authority authorizing data collection; whether disclosure is mandatory or voluntary; the purposes of use of the data; and the effects the data subject will face for non-provision of the information.[79] The Act also requires federal agencies to grant access to the data subject and provide an opportunity to correct any errors in the information.[80] The agency must then either

[74] 5 USC § 552a(a)(4). The Act defines 'record' as: 'any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or photograph.' Although the Act does not specifically mention 'biometrics' it seems quite clear that the term 'record' can include biometric applications.

[75] LK Donohue, 'Technology Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age' (2012) 97 Minn L Rev 407, esp 468-476.

[76] J Slemmons Stratford & J Stratford, 'Data Protection and Privacy in the United States and Europe' (1998) IASSIST Quarterly, esp 18.

[77] 5 USC § 552a(b).

[78] ibid While the exceptions are quite extensive, there are some safeguards built in. For example, the federal agency can disclose a record to another federal agency for civil or criminal law enforcement purposes, but only, 'if the head of the industry or instrumentality has made a written request to the agency which maintains the record specifying the particualr proportion desired and the law enforcement activity for which the record is sought.' The agency is also required to keep an accurate accounting of disclosures made.

[79] 5 USC § 552a(e)(3).

[80] 5 USC § 552a(d)(1)

correct the portion of the record or notify the individual of its refusal to do so (in which case there is an appeals process to be followed)[81] within 10 days.[82]

iii) Relevant and necessary information

38. The agency shall maintain, 'only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomophlished by statute or executive order'.[83] Further, information should be collected directly from the individual, 'to the greatest extent practicable'.[84]

iv) Data safeguarding

39. 'Appropriate administrative, technical, and physical safeguards' are required 'to insure the security and confidentiality of records and to protect against anticipated threats or hazards to their security or integrity.'[85]

CASE LAW

40 We are unaware of any cases, outside the criminal context, in which the collection and storage of biometric data has been challenged. However, the case-law below may offer some guidance.

41. In personal data cases, the Court tends to adopt a 'rational basis' review, asking whether the government has demonstrated a 'legitimate aim' and a 'rational connection' between the aim and the means used.[86] However, there is a suggestion that heightened scrutiny may apply where the personal data is especially sensitive.[87]

a) Informational privacy: constitutional challenges

i) Whalen v Roe (US Supreme Court) (1977)[88]

42. New York Statutes required physicians to report details of patients to whom they had prescribed certain drugs. The details were stored by the New York State

---

[81] 5 USC § 552a(d)(2)(B)
[82] 5 USC § 552a(d)(2)(A).
[83] 5 USC § 5552a(e)(1).
[84] 5 USC § 552a(e)(2).
[85] 5 USC § 552a(e)(10).
[86] *Iacobucci v City of Newport, Ky*, 785 F 2d 1354 (1986)
[87] *Doe v Attorney General*, 941 F2d 780 – Court of Appeals, 9th Circuit, 1991 'the more sensitive the information, the stronger the state's interest must be'.
[88] *Whalen v Roe*, 429 US 589, 97 S Ct 869, 51 L Ed 2d 64.

Department. A group of patients and doctors challenged the statute on privacy grounds The Supreme Court held the program did not pose a sufficiently serious threat to privacy to constitute a privacy violation.

43. Firstly, the Court recognised that the right to privacy included, 'an individual interest in avoiding disclosure of personal matters'.[89] Second, the Court concentrated on the 'orderly and rational' legislative process behind the New York statute.[90] Thirdly, the Court paid attention to the steps the agency had taken to prevent unauthorised disclosures of information. This enabled it to conclude that the statutory scheme 'evidence[d] a proper concern with, and protection of, the individual's interest in privacy.'[91]

44 Finally, the Supreme Court did express general concerns about privacy and emerging technologies. Mr Justice Stevens remarked,

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerised data banks or other massive government files[92]

45. Equally, Mr Justice Brennan, in a concurring opinion said,

> The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.[93]

ii) US v Westinghouse (US Court of Appeals, 3rd Cicruit) (1980)[94]

6 A subpoena granted to a health and safety inspector mandating an employer to disclose its employees' medical records was challenged as a violation of their constitutional right to privacy. The US Court of Appeals held there was no violation since: the material contained in the medical records was not 'sensitive';[95]

---

[89] ibid Stevens J at 599

[90] ibid Stevens J at 597: The New York Statute challenged in this case represents a considered attempt to deal with such a problem. It is manifestly the product of an orderly and rational and legislative decision. It was recommended by a specially appointed commission which held extensive hearings on the proposed legislation, and drew on experience with similar programs in other states.'

[91] ibid Stevens J at 605.

[92] ibid

[93] ibid 607

[94] *US v Westinghouse*, 638 F 2d 570

[95] ibid 579

effective security arrangements were in place;[96] and there was a strong public interest in allowing the health and safety inspector to have access to the medical records in this case.

47 The Court of Appeals held:

> The factors that should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorised disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognisable public interest militating toward access.[97]

48. Again, the Court issued a cautionary note about large scale data protection systems:

> Proliferation in the collection, recording and dissemination of individualised information has made the public, Congress and the judiciary increasingly alert to the threat such activity can pose to one of the most fundamental and cherished rights of American citizenship, falling within the right characterisd by Justice Brandeis as "the right to be let alone"... Much of the concern has been with the governmental accumulation of data and the ability of government officials to put information technology to uses detrimental to individual privacy, which have been facilitated by the spread of data banks and by the increasing storage in computers of sensitive information relating to the personal lives and activities of private citizens.[98]

b) Fingerprinting: constitutional challenges in the non-criminal context

i) Thom v New York Stock Exchange (Dist. Court, SD New York) (1969)[99]

49 A law requiring the fingerprinting of employees belonging to firms that carried out security exchanges was challenged on multiple grounds, including invasion of privacy. In a state level court, Edward Weinfeld DJ propounded a 'rational basis' test:

> The state having presented a valid justification...for the original taking of the prints under reasonable circumstances, their use for future identification purposes, even in criminal investigations, is not impermissible.[100]

---

[96] ibid 579-580.

[97] ibid 578. Also note *Doe v Attorney General* (n 87): 'the more sensitive the information, the stronger the state's interest must be.'

[98] ibid 576

[99] *Thom v New York Stock Exchange*, 306 F Supp 1002 (1969).

ii) Iacobucci v City of Newport, Ky (US Court of Appeals, 6th Circuit) (1986)[101]

50. A city ordinance requiring employees, at places where liquor is served, to be fingerprinted by the police was found to be constitutional. Martin CJ, citing *Thom* (above), reasoned that, 'the ordinance bears a rational relationship to a legitimate governmental interest, we view it as a proper exercise of the City's police power'.[102]

51 He then went on provide a hierarchy of protected personal information:

> Whatever the outer limits of the right to privacy, clearly it cannot be extended to apply to a procedure the Supreme Court regards as only minimally intrusive Enhanced protection has been held to apply only to such fundamental decisions as contraception...and family living arrangements. Fingerprints have not been held to merit the same level of constitutional concern.

[100] ibid 1011.
[101] Above n 86.
[102] ibid 1355.

ISRAEL

OVERVIEW

52. The Law for Including Biometric Identifying Means and Data in Documents of Identification and in Databases 2009 (the Biometric Indentification Law) was passed by the Knesset of Israel in December 2009. It provides for the embedding of biometric data (fingerprints and computerized tags of facial features) in Israeli IDs and passports, and allows for the creation of a database containing biometric data on all Israeli citizens. In addition, the data would be used by the Ministry of Interior in its future plans to create forgery-proof identification papers and passports, and allow Israeli security forces to identify and locate individuals suspected of criminal activity.

53. Despite its rhetorical appeal, opponents of the law — which includes prominent Israeli scientists and security experts — have warned that the existence of such a database risks damaging both civil liberties and state security, as any leaks could be used by criminals or hostile individuals against Israeli residents.[103]

LEGAL FRAMEWORK

54 Under Israeli law, privacy is protected by both the Basic Law: Human Dignity and Liberty 1992 (Basic Law) and the Privacy Protection Act 1981 (PPA). The Basic Law stipulates in section 7(a) that 'all persons have the right to privacy', although the right to privacy is not explicitly defined. Section 7(b)-(d) goes on to provide specific instantiations of that right:

> (b) There shall be no entry into the private premises of a person who has not consented thereto;
> (c) No search shall be conducted on the private premises of a person, nor in the body or personal effects;
> (d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.

[103] Avner Pinchuk, 'The Campaign Against the Biometric Database Act' (The Public Voice Civil Society Meeting, Jerusalem, 25 October 2010) <http://thepublicvoice.org/eventsisrael10/Avner_Pinchuk_ACRI_TPV_Meeting_Jerusalem_10_25_10.pdf> accessed 21 February 2013

55 The Israeli Supreme Court, in several key decisions,[104] has stressed that the right to privacy is a basic constitutional right, however, just like all other fundamental rights, the right to privacy is not absolute. It is subject to the 'limitations clause' in section 8 of the Basic Law, which states: 'There shall be no violation of rights under this Basic Law except by a law befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required.' These protections have effects similar to the legitimacy of purpose and proportionality tests in the European human rights and Data Protection law. Any executive or legislative action, such as the biometric database initiative, would thus be subject to this constitutional instruction.

56 The PPA forms the main element of Israeli data protection law, although it too does not define the right to privacy.[105] The PPA applies to both the private and public sector, and sets out administrative, civil, and criminal rights and obligations. Chapter 1 deals with general privacy protection: section 1 prohibits infringement of individual's privacy without that individual's consent; section 2 deals with general privacy protections, listing eleven alternative causes of action for infringement of privacy. Especially pertinent in the context of the biometric database is section 2(9). 'using, or passing on to information on a person's private affairs, otherwise than for the purpose for which it was given' (exempt from liability for 'security services'). Chapter 2 establishes a procedure for database registration, and sets forth information privacy principles which include: transparency; security; purpose limitation; confidentiality; access and rectification; and restrictions on cross-border data flows.[106] Furthermore, it defines information as 'data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.' This list, however, is not exhaustive; as the Supreme Court held in *State of Israel v Bank HaPoalim:*

> [T]he term 'information' must be interpreted in line with the legislative intent of the PPA. It should include data that can be derived from a database which is not indexed according to individual names. In other words...if financial data concerning an

---

[104] HCJ 4804/94 *Station Film Corporation Ltd. v Movie Censorship Committee*, 50(5) P.D 661, 675; CA 4463/94, 4409/94 *Golan v Prison Service*, 50(4) P.D. 136

[105] Students of the Interdisciplinary Law & Technology Workshop, *Privacy in the Digital Environment* (The Haifa Center of Law and Technology Publication Series, Publication No 7, 2005) 7.

[106] Ian Bourne, 'A Guide to Data Protection in Israel' (The Israeli Law, Information and Technology Authority January 2010) <http://www.justice.gov.il/NR/rdonlyres/C7DL2EA2-4CC2-4C51-9047-C86CC70BD50B/18333/AguiderodarLprotectionmIsraeli.pdf> accessed 21 February 2013.

individual can be derived from a database that is not indexed on a personal basis, it should be regarded as "information" under Section 7 of the PPA.[107]

57. In Israeli case law, there is no uniform definition of the right to privacy and its extent is unclear. Save for a few cases, case law has chosen not to define the right to privacy, but instead determines on a case-by-case basis whether the interests at hand form part of 'the right to privacy'.

CASE LAW

58. Since its passing, the Biometric Identification Law has drawn considerable criticism from its opponents. Most recently, in *Nahon v. Knesset*,[108] the High Court of Justice responded to a petition drafted by the Association of Civil Rights in Israel (ACRI) and the Digital Rights Movement, challenging the Biometric Identification Law and a proposed two-year 'pilot' programme.[109] The petition itself was not directed against either the use of 'smart' ID cards or the intent to embed them with biometric data; rather, it condemned the compiling of biometric identification methods and data into one central databank.[110] The Court ultimately dismissed the petition as premature, given that the pilot programme had not yet been implemented. However, the Justices strongly criticised the proposed scheme during the hearing, leading the Interior Ministry to give assurances that it would explore other options.

59. The petitioners maintained that a biometric identification system should be able to work without a central database. A central databank is neither necessary nor intended for preventing the forging of identification papers. For instance, to prevent forgeries, it would be sufficient to issue ID cards with an electronic chip (like credit cards).[111] In addition to proposing alternative solutions, the general argument was this: a databank that stores biometric data on all Israeli residents is a

---

[107] CA 86/89 *State of Israel v Bank HaPoalim*, 24(2) PD 726, 731, para 10 (5750/51-1990) as translated by Bourne (n 4)

[108] HCJ 1516/12 *Nahon v Knesset* S.CT 842 (2012) (judgment available in Hebrew) <http://elyon1.court.gov.il/files/12/160/015/c03/12015160.c03.htm> accessed 21 February 2013.

[109] Rawlson King, 'Israeli jurists right to call biometric database "extreme" and "harmful"' *BiometricUpdate.com* (30 July 2012) <www.biometricupdate.com/201207/israeli-jurists-right-to-call-biometric-database-extreme-and-harmful-> accessed 21 February 2013

[110] The Association for Civil Rights in Israel, 'Introduction from ACRI Petition to the High Court of Justice Objections to a Governmental Biometric Database' (February 2012) <http://www.acri.org.il/en/wp-content/uploads/2012/02/biometric.pdf> accessed 21 February 2013

[111] ibid

sensitive and powerful resource that has the potential to become an unparalleled mechanism for surveillance and control, resulting in both direct and indirect breaches to constitutional rights (e.g. right to dignity, liberty and privacy).

60 During the hearing, the Justices of the High Court were harshly critical of the Israeli's government biometric scheme. In particular, they were not convinced that the government would have to maintain a central database given that smart identification cards can be issued without one.[112] Given the other security infractions that have occurred with Israeli biometric systems in the past (e.g. theft of biometric data for nine million Israeli citizens in 2006), the High Court demanded that the Interior Ministry rework its planned pilot of the program to evaluate whether it is actually *necessary* to store the population's biometric data in a single, centralized database. Since then, the Interior Ministry has been exploring other options, as well as evaluating safeguards to limit the possibility of data leaks and information theft.[113]

61. Other cases, of particular relevance to the biometric data scheme, include the following:

a. In *Plonit (Jane Doe) v National Rabbinical Court* (2006), the Israeli Supreme Court held that the right to privacy is not only one of the most important fundamental rights, but it plays a vital role in shaping the democratic character of Israel's legal system. These decisions were reiterated in *Rami Mor v Barak ETC* (2010)—a case in which the Supreme Court refused to order that an Internet service provider unmask a John Doe defendant — by holding that the constitutional right to privacy entails a right *to anonymity*.[114]

b. In *Association for Civil Rights in Israel v Minister of Interior* (2004), the Israeli Supreme Court ruled that the data sharing practices within the public sector, while authorized by statute, were unconstitutional. The data transfers were considered overly broad, which in turn had a disproportionate effect on an individual's privacy rights. The court ruled that data transfers must be restricted by regulations specifying the uses of data, its users and security measures.

---

[112] King (n 109)
[113] The Association for Civil Rights in Israel (n 110).
[114] LCA 4447/07 *Rami Mor v. Barak E.T.C the Company for Bezeq International Services Ltd* (2010) as translated by Google Translate < http://elyon1.court.gov.il/files/07/470/044/p10/07044470.p10.htm> accessed 21 February 2013

Moreover, it specified that the transfer of data between government officials and private sector financial institutions must be authorized explicitly through primary legislation; in this case, anti-money laundering provisions in secondary regulations did not suffice.[115]

[115] HCJ 8070/98 *ACRI v Ministry of Interior*, 58(4) S.CT 842 (2004) as translated by Google Translate <http://elyon1.court.gov.il/files/98/700/080/I09/98080700.I09.htm>.

AUSTRALIA

OVERVIEW

62 The Australian Constitution does not contain a right to privacy, or any similar right, and no such rights have been found to be implied in the Constitution. There is no federal bill of rights and no general right to privacy has been recognised in the common law. As a result, privacy is protected through legislation, principally the Privacy Act 1998 (Privacy Act).

63. Legislation to create a national identity system — the 'Australia Card' — which would have amalgamated all government identification systems into a single database, was introduced in the 1980s, but abandoned due to strong public opposition.[116] No subsequent government has shown serious interest in revisiting the concept and even comparatively limited proposals, such as a consolidated healthcare access card, have been rejected. Specific biometric systems are widely used by the government, such as for 'ePassports', and by private bodies, such as nightclubs, which collect biometric information as a condition of entry, typically for the purpose of identifying troublemakers.[117] The Privacy Act regulates these systems.

LEGAL FRAMEWORK

64. The principal protection for privacy in Australia is the Privacy Act. It operates alongside a set of overlapping, complex and potentially contradictory[118] federal and state/territory statutes that address specific aspects of privacy law, such as telecommunications.

65 The Privacy Act was introduced in order to implement the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and Australia' s obligations under Article 17 of the International Covenant on Civil and Political

[116] Graham Greenleaf, 'The Australia Card – deux ex machine?' (1998) 3(6) Computer Law & Security Report 6.
[117] Biometrics Institute, 'Where are biometrics used' <http://www.biometricsinstitute.org/pages/faq-3.html> accessed 21 February 2013
[118] Australian Law Reform Commission, 'Review of Australian Privacy Law, Discussion Paper No 72 '(2007) 328–9.

Rights.[119] It was initially designed only to protect personal information in the possession of federal government departments, but was subsequently extended to apply information in the possession of most private parties.

66. The Privacy Act regulates how information is collected, used, disclosed and kept.[120] Government agencies must take reasonable steps to protect personal information against loss, unauthorised access, modification, use or disclosure, and other misuse. These obligations are expressed in general terms, for example to ensure that there are 'such security safeguards as it is reasonable'.[121] The Privacy Act requires that 'sensitive information' be managed with particular care. Sensitive information, generally, can only be collected with a person's consent and only disclosed for limited reasons.[122] In December 2012 biometric information was added to the list of material classified in the Privacy Act as 'sensitive information' by statutory amendment.[123] The list of 'sensitive information' also includes, among other things, information or opinion about a persons racial or ethnic origin, religious affiliations, philosophical beliefs, sexual preferences and criminal record.[124]

67. The operation of the Privacy Act is overseen by the Office of the Australian Information Commissioner (OAIC), an independent statutory body. While the OAIC has been active in investigating complaints, it has not considered a challenge to the existence of government databases containing personal information. It would not have the power to do so if such databases were established by legislation. The OAIC's function is limited to the specific powers granted to it under statute, which are to ensure that existing legislation is complied with, rather than to evaluate new legislation.[125]

---

[119] Office of the Australian Information Commissioner, 'History' <http://www.privacy.gov.au/aboutprivacy/history> accessed 21 February 2013

[120] Privacy Act 1988, s 14.

[121] Privacy Act 1988, s 14 Principle 4

[122] Privacy Act 1998, Schedule 3, National Privacy Principle 10

[123] The amendment was made by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, Schedule 1, s 42

[124] Privacy Act 1998, s 6(1), 'sensitive information'

[125] Australian Information Commissioner Act 2010, s 9.

CASE LAW AND POLITICAL DEBATE

133

68. There is no Australian case law in which a superior court has recognised a right to privacy in the Constitution or in the common law.[126] In *ABC v Lenah Game Meats* the High Court left open the possibility that such a right might develop in the common law,[127] but, even if it did, such a common law right could be overridden by legislation.

69 The OAIC, (and its predecessor the Australian Privacy Commissioner) investigates complaints about government and private bodies that may be in breach of the Privacy Act[128] and conducts audits of bodies that hold significant amounts of private data,[129] but its powers are limited to ensuring compliance with the existing legislation.

70 In 1985 the Australian Federal Government proposed a national identity card and associated database, which was intended to reduce benefit fraud, tax fraud and to control illegal immigration.[130] It ultimately abandoned the proposal in the face of sustained public opposition and criticism, primarily on privacy grounds.[131] In 2006 the Federal Government tabled legislation for a single health care and social services access card, to replace 17 existing government issued cards.[132] The bill was withdrawn in 2007 after a Senate inquiry harshly criticised the proposal on the basis of poor drafting and inadequate protections for privacy.[133] The inquiry expressed concern about the proposal generally:[134]

---

[126] *Victoria Park Racing & Recreation Grounds Co Ltd v Taylor* [1937] HCA 45, (1937) 58 CLR 479.

[127] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63, 208 CLR 199. Such a right has been asserted in two lower state court decisions, but they have never been followed by higher courts *Doe v ABC* [2007] VCC 281 and *Grosse v Purvis* [2003] QDC 151

[128] *For* example *J and Commonwealth Agency* [2011] AICmrCN 4.

[129] See for example Office of the Australian Information Commissioner, Audit of the National Document Verification Service, Centrelink, June 2011 <http://www.oaic.gov.au/publications/reports/audits/document_verification_service_audit_report.html> accessed 21 February 2013

[130] Australian Parliamentary Library 'Identity Cards and the Acceess Card,' 17 August 2010 <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards> accessed 21 February 2013

[131] Greenleaf (n 116) 6.

[132] Australian Parliamentary Library 'Identity Cards and the Acceess Card,' 17 August 2010 <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards> accessed 21 February 2013

[133] Senate Standing Committees on Finance and Public Administration, Report into the Human Services (Enhance Service Delivery) Bill 2007, 15 March 2007, see especially Chapter 3

[134] Senate Standing Committees on Finance and Public Administration, Report into the Human Services (Enhance Service Delivery) Bill 2007, 15 March 2007, 3 89

> The register gives rise to the prospect of the government having unprecedented access to a single national database containing the majority of Australia's adult population's basic personal information. It is seen as presenting a major risk to personal privacy and security, not only from government agencies but also other parties with malicious intent.
> ...
>
> [In a historical context] [n]o previous Australian government, even in wartime, has effectively required all its citizens to give it a physical representation of themselves, nor contemplated having this stored in one national database

However, there was no suggestion that the Australian Parliament lacked the power to introduce the legislation, simply that it would be unwise to do so.

135

COUNCIL OF EUROPE

OVERVIEW

71 The European Court of Human Rights (ECtHR) adjudicates the compatibility with the European Convention on Human Rights[135] (ECHR) of Council of Europe Member States' national measures, including privacy legislation. The ECtHR therefore ensures that national biometric identification systems are consistent with the human rights norms enshrined in the ECHR, which include the right to respect for private life.

LEGAL FRAMEWORK

a) Article 8 ECHR

72. The legal framework for privacy protection under the jurisdiction of the ECtHR centres upon Article 8 ECHR. Article 8(1), so far as relevant, states that: 'Everyone has the right to respect for his private... life'.

73 Article 8(2) states:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

74 Article 8(1) ECHR therefore protects the right to privacy. Article 8(2) lists exhaustively the circumstances in which limitations on the right may be considered justified. The right can be limited in pursuance of a number of legitimate aims which may be relied on by a public authority acting in accordance with law and only so far as is necessary in a democratic society. It is for the public authority in each case to demonstrate that the measure which constitutes an interference with the

[135] Convention for the Protection of Human Rights and Fundamental Freedoms 1950.

right to private life is in accordance with law, serves a legitimate aim and is proportionate to the achievement of that aim.[136]

b) Data Protection Convention

75. The Council of Europe has also produced a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Data Protection Convention).[137] The ECtHR is not entitled to interpret this Convention as it is entitled to interpret the ECHR, however the Court does refer to the Data Protection Convention in its case law to guide its interpretation of the notion of private life in Article 8 ECHR. The purpose of the Data Protection Convention is to extend the safeguards of the right to privacy in relation to personal data undergoing automatic processing.[138] 'Personal data' is defined in the Data Protection Convention as 'any information relating to an identified or identifiable individual'.[139] The Explanatory Report[140] clarifies that 'automatic data processing' is capable of a flexible interpretation[141] and includes electronically processed data, but not data which is merely collected.

76. States Parties have a duty to take the necessary measures in their domestic legislation to give effect to the principles of data protection set out in the Convention in order to ensure respect in their territory for the fundamental human rights of all individuals as regards the processing of personal data.[142] For example, sensitive data may not be processed automatically unless domestic law provides appropriate safeguards. The categories of sensitive data under the Convention include personal data 'revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [and]... relating to criminal convictions'.[143] States must take appropriate security measures for the protection of personal data stored in automated data files.[144]

---

[136] On the application of proportionality in the context of Article 8 ECHR, see Harris, O'Boyle and Warbrick, *Law of the European Convention on Human Rights* (2nd edn, OUP 2009) Ch 9, 407-422.
[137] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (Data Protection Convention)
[138] ibid Preamble.
[139] ibid art 2(a).
[140] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 – Explanatory Report <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm> accessed 21 February 2013
[141] ibid [31]
[142] Data Protection Convention, art 4.
[143] ibid art 6
[144] ibid art 7.

77. The Explanatory Report expounds that the principles enshrined in the Data Protection Convention are intended to be universal and not limited to a European context.[145] The ECtHR refers to the Data Protection Convention in its case law to assist with the interpretation of the right to respect for private life under Article 8 of the ECHR.

CASE LAW

78 The landmark ECtHR case on the retention of biometric information and the right to respect for private life is *S and Marper v United Kingdom*.[146]

79. The applicants were arrested and charged with criminal offences. Fingerprints and DNA samples were taken from them under section 64 of the Police and Criminal Evidence Act 1984. One of the applicants was acquitted and the case against the other was discontinued. The applicants requested the destruction of their fingerprints, cellular samples and DNA profiles held by the police, but this was denied. At national level, the House of Lords rejected the applicants' appeal against the decision not to destroy the data.[147] The applicants complained to the ECtHR that the retention of their fingerprints, cellular samples and DNA profiles after the acquittal/discontinuance of their case was inconsistent with the right to respect for private life enshrined in Article 8 ECHR.

80. The Grand Chamber of the ECtHR held that the concept of 'private life' is a broad term, not susceptible to exhaustive definition, and includes means of personal identification.[148] All forms of information retained in the instant case were held to fall within the meaning of 'personal data'.[149] The Court concluded that retention of each type of data amounted to an interference with the right to respect for private life under Article 8 ECHR.[150]

81 Given the nature and amount of personal information contained in the cellular samples, their retention per se was regarded as interfering with the right to respect

---

[145] Data Protection Convention Explanatory Report [24] and [90]
[146] *S and Marper v UK* (2009) 48 EHRR 50
[147] *R (on the application of S) v Chief Constable of South Yorkshire* [2004] UKHL 39, [2004] 1 WLR 2196.
[148] *S and Marper* (n 146) [66].
[149] ibid [68].
[150] ibid [73], [75] and [86]

for the private lives of the individuals.[151] The DNA profiles, as sensitive data containing much information relating to personal identification, revealing racial origin or matters of health, attracted a heightened level of protection.[152] As regards retention of fingerprint data, the Court revisited prior ECHR jurisprudence. Whether the taking of fingerprints constituted an interference with the right to respect for private life was left open in *McVeigh*.[153] In *Kinnunen v. Finland*[154] the European Commission on Human Rights held that retention did not constitute an interference with the Article 8 right. However, the ECtHR considered it appropriate to review this issue in light of subsequent developments in the law relating to the processing of photographs[155] and voice sample data.[156] In relation to retention of photographs, the holding in the *Friedl* case that there was no interference with the Article 8 right was based to a significant extent on the fact that the photographs were not entered into any data processing system, which suggests that whenever photographs are retained and processed, there will be an interference with Article 8. The taking of voice samples by police in *PG v UK*[157] was held to constitute an interference with the right to respect for private life. The Court in *S and Marper* concluded that retention of fingerprints could in itself give rise to important private life concerns[158] and constituted an interference with the right to respect for private life.

82. These conclusions were ultimately reiterated and reinforced:

> [T]he mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.[159]

The Court accepted that the retention of the applicants' fingerprint and DNA records had a clear basis in domestic law.[160] The Court also accepted that the

---

[151] ibid [72].
[152] ibid [76]
[153] *McVeigh, O'Neill and Evans v UK* (1983) 5 EHRR 71.
[154] *Kinnunen v Finland*, no 24950/94, Commission decision of 15 May 1996
[155] *Friedl v Austria* (1996) 21 EHRR 83.
[156] *PG v UK* (2008) 46 EHRR 51.
[157] (2001) 31 EHRR 1016.
[158] *S and Marper* (n 146) [85].
[159] ibid [121].
[160] ibid [97]

retention of fingerprint and DNA data pursed the legitimate purpose of the detection and prevention of crime[161].

83. However, the ECtHR held that the interference with the right to respect for private life by the retention of this data was not justifiable as necessary in a democratic society[162]. The Court referred to the importance of the privacy interest in data protection:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private... life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned... The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse...

The intrinsically private character of the information taken from the applicants called for the Court to exercise careful scrutiny of State measures relating to the retention and use of such data.

84. The Court placed weight on the fact that the UK was the only Member State of the Council of Europe which permitted indefinite retention of fingerprint and DNA data.[163] It compared the practice of the majority of other Member States, which required such samples to be removed or destroyed either immediately or within a certain time after acquittal or discharge.[164] The blanket and indiscriminate nature of its powers of retention meant that the UK had overstepped its margin of appreciation and failed to strike a fair balance between the competing public and private interests. Accordingly, the retention of the applicants' data was a disproportionate interference with their right to respect for private life and a constituted a violation of Article 8 ECHR.[165]

---

[161] ibid [100] and [117].
[162] ibid [125]
[163] ibid [110]
[164] ibid [108]
[165] ibid [125]

85 The Grand Chamber's approach in *S and Marper v UK* therefore indicates that a national system of collection and retention of biometric information must incorporate sufficient safeguards in order adequately to protect the right to respect for private life. It appears that by 'appropriate safeguards', the Court means that the law must include requirements against indefinite storage and that retention must not be excessive in terms of coverage, i.e. overly inclusive as regards whose data is to be stored.

EUROPEAN UNION

OVERVIEW

86. The European Union has enacted Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.[166] This was amended by Council Regulation (EC) 444/2009 of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel document issued by Member States. This introduces passports and travel documents that contain biometric data, namely facial image and two fingerprints taken flat in interoperable formats.[167]

LEGAL FRAMEWORK

a) Charter on Fundamental Rights of the European Union

87 The Charter has the same legal value as the Treaties.[168] Article 7 guarantees respect for private and family life and Article 8 guarantees the protection of personal data. Limitations may be imposed on Articles 7 and 8, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest.[169]

b) European Convention of Human Rights (ECHR)

88. The rights in the ECHR, including Article 8,[170] constitute general principles of Union law.[171] Also, where Charter rights correspond to Convention rights, the meaning and scope of those rights are to be the same as those laid down by the Convention[172] and nothing in the Charter is to be interpreted as restricting or adversely affecting the rights recognised by the Convention.[173]

---

[166] Regulation 2252/2004 of 13 December 2004 [2004] OJ L385/1
[167] ibid art 1(2)
[168] Treaty on European Union, art 6(1)
[169] Charter on the Fundamental Rights of the European Union, art 52(1)
[170] Which protects the right to respect for private and family life, home and correspondence See above para 72-75
[171] Treaty on European Union, art 6(3)
[172] Charter on Fundamental Rights of the European Union, art 52(3)
[173] ibid art 53

c) Council Directive 95/46/EC[174]

89. The Directive deals with 'personal data' which is defined in Article 2(a) as 'any information relating to an identified or identifiable natural person'. The Working Party,[175] which gives opinions to the European Commission on Union laws affecting the right to privacy, has concluded that biometric data would fall into this category since '[i]n the context of biometrical identification, the person is generally identifiable, since the biometric data are used for identification or authentication/verification at least in the sense that the data subject is distinguished from any other.'[176]

90. Article 8 provides extra safeguards for 'sensitive data', defined as data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . health or sex life'.[177] The Working Party identifies that biometric systems could classified as 'sensitive information' where the system is based on face recognition, which would reveal ethnic or racial origin.[178]

91. Together Article 6(1)(b) and 6(1)(c) require that the collection of data should be tightly linked to the purpose and should not be excessive in relation to the purpose. However, Article 13 does allow for derogation from this, and other specified obligations and rights.[179]

92. The Preamble and Article 1(1) state that the right to privacy is to be respected. The safeguards provided for, give a number of rights to the data subject, including the right to information[180], right of access[181] and right to object[182]. There are guarantees

---

[174] Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[175] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, which was set up by section 29 of Directive 95/46. The Working Party is comprised of representatives from data protection authorities in all EU Member States, the European Data Protection Supervisor, and a representative of the EU Commission.

[176] Working Party, 'Working Paper 80· Working document on biometrics' (2003) 12168/02/EN [section 3.1]

[177] Council Directive 95/46/EC, art 8(1).

[178] Working Party, 'Working document on biometrics' (n 176) 10.

[179] Allows derogations from Articles 6(1), 10, 11(1), 12 and 21 of Directive 95/46

[180] Council Directive 95/46/EC, arts 10 and 11.

[181] ibid art 12.

[182] ibid arts 14 and 15

relating to data quality[183] and consent[184]. Also, the Directive lays down security measures[185], notification obligations[186] and prior checking.[187]

d) Council Regulation (EC) 2252/2004[188]

93. The two aims of the scheme, specified in Article 4(3), are to verify the authenticity of the document and the identity of the holder by means of directly available comparable features. This serves the overall aim of combating falsification and fraudulent use of passports and other travel documents issued by the Member States.

94. Recital 8 of the Preamble states that the protection for 'personal data' in Directive 95/46 still applies. There are extra safeguards provided in the Regulation. Article 1(2) provides that the data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. Article 4(1) gives a right to the data subject to verify and rectify, and Article 2 lays down technical specifications. The amendments in Regulation 444/2009 introduce Article 1a which requires qualified and authorised staff. The amendments also require compliance with international standards.[189]

CASE LAW AND POLITICAL DEBATES

95. Two Member States have referred questions to the European Court of Justice (ECJ) concerning the validity of Regulation 2252/2004. These are on the docket of the ECJ and are pending decision. The ECJ has not decided a case concerning biometric information before.[190] However, the ECJ has ruled on the right to the protection of personal data in general (noted below).

---

[183] ibid art 6
[184] ibid art 7.
[185] ibid art 17.
[186] ibid art 18
[187] ibid art 20
[188] Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L385/1.
[189] This includes the ECHR, UN Convention on the Rights of the Child and the International Civil Aviation Organisation
[190] The ECJ has ruled on Regulation 2252/2004 before, in C-137/05 United Kingdom of Great Britain and Northern Ireland v Council of the European Union [2007] ECR I-11593, but this concerned the validity of the Regulation The UK complained that the Regulation should be annulled because they did not take part in its adoption The ECJ decided that the Regulation was valid The specific issue of biometric data was not discussed.

a) Dutch preliminary reference

96 Firstly, the Dutch Council of State (*Raad van State*, the highest Dutch administrative court) referred the question to the ECJ whether the requirement of fingerprints in passports violates citizens' right to privacy.[191] This referral concerns four separate cases, where three Dutch citizens were denied passports and another citizen was denied an ID card for refusing to provide their fingerprints. The Dutch Council questions whether Article 1(2) of the Regulation is valid in the light of Articles 7 and 8 of the Charter, and Article 8 ECHR. They also question whether, if Article 1(2) is valid, this means that Article 4(3), in the light of Articles 7 and 8 of the Charter and Article 8 ECHR, must be interpreted as meaning that it should be guaranteed by legislation that the biometric data, must not be collected, processed and used for purposes other than the issuing of the document. This latter issue, concerning the purpose of the data, raises similar issues to that dealt with by the French Conseil Constitutionel.[192]

b) German preliminary reference

97. Secondly, a German Administrative Court (Gelsenkirchen District Administrative Court) has also referred a question to the ECJ concerning the Regulation.[193] This case involves a German citizen who was not issued a new passport because he refused to give his fingerprints. The German Court questions whether Article 2(1) is valid.[194]

c) C-139/01 Österreichischer Rundfunk and Others [2003] E.C.R. I-4989

98 The ECJ has decided cases on Directive 95/46 and the right to protection of personal data in general Österreichischer Rundfunk concerned provisions of Austrian law which required public bodies subject to control by the Rechnungshof (Court of Auditors) to communicate to it the salaries and pensions exceeding a certain level paid by them to their employees and pensioners, together with the

[191] Case C-446/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 3 October 2012 — W.P Willems; other party. Burgemeester van Nuth, Case C-447/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 5 October 2012 — H.J Kooistra; other party: Burgemeester van Skarsterlân, Case C-448/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 8 October 2012 — M Roest; other party: Burgemeester van Amsterdam; Case C-449/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 8 October 2012 — L.J.A. van Luijk; other party: Burgemeester van Den Haag

[192] Décision n° 2012-652 DC du 22 mars 2012

[193] Case C-291/12 Reference for a preliminary ruling from the Verwaltungsgericht Gelsenkirchen (Germany) lodged on 12 June 2012 — Michael Schwarz v Stadt Bochum

[194] See further Germany, n 238 below.

names of the recipients. The ECJ held that the Directive had necessarily to be interpreted in the light of fundamental rights, in particular the right to privacy.[195] To establish an interference with the right to privacy, it was sufficient to find that data had been communicated by the employer to a third party.[196] The Court stated that 'the question was whether stating the names of the persons concerned in relation to the income received is proportionate to the legitimate aim pursued and whether the reasons relied on before the Court to justify such disclosure appear relevant and sufficient.'[197] The Court noted that there should be an examination as to whether the objective of keeping salaries within reasonable limits could have been attained effectively by transmitting the information as to names to the monitoring bodies alone. Similarly, the question arose whether it would have been sufficient to inform the general public only of the remuneration and other financial benefits to which persons employed by the public bodies concerned had a contractual or statutory right, but not of the sums which each of them actually received during the year in question.[198] However, the ECJ did not reach a final conclusion and the issue was left up to the Member State to decide.[199]

99 This case was followed by the ECJ in Joint cases C-92/09 and C-93/09 Volker und Markus Schecke GbR v Land Hessen; Eifert v Land Hessen;[200] where the ECJ stated that '[i]n relation to proportionality, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.'[201]

[195] C-139/01 Österreichischer Rundfunk and Others [2003] E.C.R. I-4989 [68].
[196] ibid [75]
[197] ibid [86]
[198] ibid [88]
[199] ibid [94]
[200] [2010] ECR I-nyr
[201] Joint cases C-92/09 and C-93/09 Volker und Markus Schecke GbR v Land Hessen, Eifert v Land Hessen; [2010] ECR I-nyr [77].

UNITED KINGDOM

OVERVIEW

100. There is no general 'right to privacy' under UK law. As a result, the courts, using Article 8 ECHR as their basis, have striven to develop the common law to afford adequate protection to privacy interests.[202] In addition to this, there are a number of discrete statutes addressing a range of privacy concerns, the most relevant of which is the Data Protection Act 1998 [203]

101 Since the government's ultimately unsuccessful attempt to introduce an identity card scheme (complete with biometric data) in 2006, the legislative trend has shifted towards greater protection of sensitive information — a movement typified by the recent Protection of Freedoms Act 2012.

LEGAL FRAMEWORK

102 Although there is no overarching right to privacy in the UK, domestic judicial and legislative intervention and laws enacted at European level have begun to fashion a piecemeal protection of sorts. Article 8 of the ECHR, incorporated into UK law by the Human Rights Act 1998,[204] states that everyone has the right to respect for their private and family life. It is evident that in some circumstances this respect may be infringed by the collection and storage of biometric data. In such circumstances, those responsible for the storage must justify the interference in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime, or for the protection of the rights of others (as per the permissible limitations of the right in article 8(2) ECHR).

103. Further to this, the Data Protection Act 1998 regulates the storage and use of 'personal data', which the Act defines as data relating to a living individual who can be identified from those data, or from a combination of those data along with other

[202] See *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22.
[203] Data Protection Act 1998 <http://www.legislation.gov.uk/ukpga/1998/29/contents> accessed 21 February 2013
[204] Human Rights Act 1998 <http://www.legislation.gov.uk/ukpga/1998/42/contents> accessed 21 February 2013.

information which the data controller has, or is likely to have.[205] The Act applies to any individual or organisation that 'determines the purposes for which and the manner in which any personal data are, or are to be, processed'.[206] Schedule 1 of the Act outlines eight key features,[207] which must be considered by any such individual or organisation. The most relevant, for the purposes of biometric information, are that data must be fairly and lawfully processed,[208] obtained for one or more specified and lawful purposes,[209] not kept for longer than is needed for these purposes,[210] and stored with appropriate security.[211] Indeed, where the data concerned consists of information as to, inter alia, an individual's racial or ethnic origin, alleged criminal history, or physical or mental health, then it will be considered sensitive and deserving of an even higher level of protection in its processing and storage[212]. Exemptions from the Act are available in a number of circumstances, including when compliance with the Act would fetter crime prevention[213] or risk national security[214]. Further exemptions arise where the Act might hamper functions — whether of a public nature, conferred by enactment on any particular body, or carried out by government — that are designed to protect the public against maladministration, financial loss or malpractice.[215] Finally, data processors that process information for the purposes a public register may be exempted from the requirement to notify the Information Commissioner.[216]

104. In addition, the government has recently introduced the Protection of Freedoms Act 2012[217] 'to restore the rights of individuals in the face of encroaching state power, in keeping with Britain's tradition of freedom and fairness'. The Act regulates the destruction, retention and use of fingerprints, footwear impressions and DNA samples and tightens up the relatively weak protections, formerly offered in the Police and Criminal Evidence Act 1984. Notable safeguards within the 2012

---

[205] Data Protection Act 1998, Section 1(1)
[206] ibid.
[207] Data Protection Act 1998, Schedule 1, Part 1.
[208] ibid Schedule 1, Section 1
[209] ibid Schedule 1, Section 2
[210] ibid Schedule 1, Section 5
[211] ibid Schedule 1, Section 7
[212] ibid Schedule 3
[213] ibid Section 29
[214] ibid Section 28(1)
[215] ibid Section 31.
[216] ibid Section 17(4)
[217] Protection of Freedoms Act 2012 <http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted> accessed 21 February 2013

Act include: the requirement that fingerprints and DNA taken from a person arrested for or charged with a minor offence are destroyed following a decision not to charge or an acquittal; the availability of only limited grounds upon which periods of retention may be extended; and the appointment of a Commissioner for the Retention and Use of Biometric Material, with powers of review, including the power to order destruction of information where it is deemed that the criteria for extended retention have not been met. Although commentary on the Act's effectiveness must be necessarily tentative, due primarily to its infancy, its introduction represents an acceptance of the need to treat biometric information with particular sensitivity and shows a willingness on the part of the UK government to comply with the ruling of the ECtHR in *S and Marper v UK*, which considered that the UK's former policy of DNA retention constituted a 'disproportionate interference with the applicants' right to respect for private life'.[218]

105. Finally, there is an independent regulatory authority — the Information Commissioner's Office — that deals principally with oversight of the Data Protection Act 1998. The role of this body is to monitor organisations and individuals that collect, use and keep personal information and ensure that their procedures accord with the statutory requirements. The Commissioner has the power to initiate criminal prosecutions and can also pursue avenues of non-criminal enforcement, audit, and impose monetary penalties of up to £500,000 for statutory infringements.

CASE LAW AND POLITICAL DEBATE

106. The movement in favour of the UK identity card stems back to the late 1990s when Labour Minister Jack Straw first proposed the idea of 'citizen's access card'. Following the September 11th attacks in the USA and the July 7th attacks in London, the notion that ID cards could offer valuable assistance in the fight against terrorism grew in popularity. The momentum of this argument gradually faded, and by the time the Identity Card Act 2006 came into force it was being justified primarily on the grounds that it would combat identity theft, help prevent illegal

[218] *S and Marper v UK* (n 146) [125].

immigration, and help people to prove their identities more easily when travelling, opening bank accounts and renting property.

107 The enabling legislation gave the government considerable discretion as to how the scheme was to be implemented. The eventual model involved a physical card that linked back to the national identity database, which contained information such as photographs, national insurance numbers, dates of birth, addresses, and biometric information, such as fingerprints. The scheme was compulsory for non-EU migrants and workers in high-risk areas, but was, at least theoretically, voluntary for the general population. In effect, however, given that it was impossible to renew travel documents without registering on the database, the scheme was de facto compulsory for the vast majority.

108. By the time the bill had worked its way to Parliament, opposition from many quarters had hardened. For instance, the then Foreign Secretary, Jack Straw, warned that the pursuance of the ID card policy was "deeply flawed". Despite further notable objections, including the scheme being condemned as 'compulsion by the backdoor' in the House of Lords debates[219] and a report by the London School of Economics suggesting that the costs of such a scheme would be unsustainable[220], the Bill passed by a narrow margin.

109 From its inception, the scheme faced further resistance, with the Conservatives and Liberal Democrats promptly announcing their defiant opposition to it. A report produced by 'Liberty' - an independent campaigning organisation working to promote civil liberties and human rights - opposed the scheme for its far-reaching implications 'on the relationship between the individual and the state' and expressed concerns regarding the aggregating of information streams which, although potentially innocuous when kept apart, were significantly more intrusive when amalgamated[221]. Further challenges on privacy grounds came from the Information Commissioner, Richard Thomas, who cautioned that the introduction of identity cards 'fundamentally changed the relationship between state and

---

[219] House of Lords Debate <http://www.parliament.the-stationery-office.co.uk/pa/cm200506/cmhansrd/vo060213/debtext/60213-24.htm> accessed 21 February 2013.
[220] LSE, 'The Identity Report' <http://is.lse.ac.uk/idcard/identityreport.pdf> accessed 21 February 2013.
[221] Liberty's response to the draft bill <http://www.liberty-human-rights.org.uk/pdfs/policy04/id-card-draft-bill-response.pdf> accessed 21 February 2013

citizen'[222]. The Commissioner also expressed worries about the digital trail that would be left by the central logging of every ID check and pointed out that the register could act as a detailed log of individuals' activities and transactions.

110. In light of the staunch and persistent criticism, it is, perhaps, unsurprising that the first bill to pass through Parliament under the new Conservative-Liberal Democrat coalition government, was one which entirely reversed the effects of the Identity Card Act 2006 for UK citizens - the Identity Documents Act 2010. The 2010 Act did, however, retain the scheme of biometric residence permits in place for non-EU nationals, although these permits continue to be issued pursuant to different legislation and the information gathered is not stored on the (now abolished) national identity register.

[222] ICO report into Identity Cards <http://www.ico.gov.uk/upload_documents/library/corporate/detailed_specialist_guides/id_cards_bill_-_ico_concerns_october_2005.pdf> accessed 21 February 2013

FRANCE

OVERVIEW

111 The right to privacy enjoys constitutional as well as statutory protection in France. The French constitutional court, the *Conseil Constitutionnel Français*, interprets Article 2 of the French Constitution as implicitly including the right to privacy ('*le droit au respect de la vie privée*') which extends to the protection of personal data.[223] France adopted a general data protection law, Act 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties,[224] long before the European Union Directive on data protection.[225]

LEGAL FRAMEWORK

a) Constitutional protection

112. The *Conseil Constitutionnel Français* (hereafter: *Conseil*) has the power to strike down laws of the Parliament incompatible with the Constitution. The *Conseil* mainly exercises *a priori* judicial review, i.e. before the final promulgation of laws. Since the 2007 constitutional reform, the *Conseil* can also strike down laws of Parliament that have already been promulgated if a regular court refers the constitutional question to the *Conseil*.

b) Statutory Protection

113 The Act 78-17 of 6 January 1978 on Data processing, Files and Individual Liberties set up an independent administration authority, the Commission nationale de l'informatique et des libertés (CNIL). The CNIL serves as the national data protection agency under the 95/46 EC Directive.[226] It issues opinions on legislation concerning data protection. The CNIL is discussed in further detail below.

---

[223] Article 2 of the Declaration (secod sentence): '*These rights are liberty, property, security, and resistance to oppression.*' It is worth highlighting that due to the ancient nature of the text, the majority of rights are intrepreted from abstract rights included in Article 2. Hence, the right to privacy enjoys the status of a ful-blooded constitutional right, it does not merely remain in a penumbra of other rights.

[224] The Act 78-17 of 6 January 1978 on Data processing, Files and Individual Liberties.

[225] See above paras 89-92.

[226] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

CASE LAW

114 This section discusses one recent high profile precedent and includes further decisions concerning the treatment of biometric information by law enforcement agencies.

a) Décision n° 2012-652 DC du 22 mars 2012[227]

115. MPs requested the *Conseil Constitutionel* to review the constitutionality of national identity card legislation that aimed to introduce a new ID card with an electronic chip that included biometric information (face image and fingerprints) and established a national database for this information.[228] The alleged aim of the law was to fight against identity fraud. The petition argued that the scheme breached the right to privacy. The *Conseil* struck down part of the law, namely its Article 5 and 10.[229]

116. The *Conseil* began by stating that 'the right to respect for private life; that accordingly, the collection, registration, conservation, consultation and communication of personal data must be justified on grounds of general interest and implemented in an adequate manner, proportionate to this objective.'[230] It scrutinised four aspects of the law: (a) the size of the database, that potentially covered the whole population; (b) biometric data, namely fingerprints as particularly sensitive data because of their immutable nature; (c) the means proposed to achieve the aim of the law; (d) the plurality of the ends that the database was to serve according to the law. The court found that the Act served a legitimate aim, i.e. fighting against identity fraud, though the scheme was to be found disproportionate. The *Conseil* found that on the one hand the databases was broad in coverage included particularly sensitive data, on the other hand police and other judicial authorities were explicitly granted access to the database in cases unrelated to the original purpose of the law, i.e. the prevention of fraud.[231] The *Conseil* found it disproportionate even though the consultation of the database was

---

[227] Official English translation available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil_constitutionnel_105428.pdf> accessed 21 February 2013.

[228] Loi du 6 mars 2010 relative à la protection de l'identité (Identity Protection Act).

[229] This decision also had another prong on the commercial, private use of the chip that was struck down on different grounds, and it is irrelevant for this issue

[230] Décision n° 2012-652 DC du 22 mars 2012 [8]

[231] ibid [10]. 'that the technical characteristics of this database as defined by the contested provisions enable it to be consulted for purposes that other than the verification of an individual's identity '

'for investigative requirements relating to certain offenses if authorized by the public prosecutor or the examining judge'.[232] It should be noted that the *Conseil* did not take issue with the creation of a population-wide biometric database per se.

117. It is worth mentioning that the CNIL, the national data protection agency, also scrutinised the legality of the national database.[233] The CNIL held the legislator to higher standard when finding the law to be a disproportionate restriction on the right to privacy. According to the CNIL the legislator did not use the least restrictive means to achieve the legitimate aim with the same efficiency, hence the scheme amounted to a disproportionate restriction of the right to privacy. The CNIL stipulated that the fight against identity fraud did not compel the government to set up such a broad-scale biometric database. It held that a one-way identification system ('match on card') would have been equally effective in achieving the aim. The *Conseil Constitutionel* therefore showed more deference to the legislature in this respect.

b) Database maintained by the police and further law enforcement agencies

118. The *Conseil Constitutionel* has reviewed a number of other databases from the perspective of the right to privacy. Among them there are two that explicitly deal with biometric information. According to the official commentary issued by the *Conseil Constitutionel*, there is a greater threat to the right to privacy where databases are run for private purposes and if the purpose served by database falls outside the scope of criminal offenses.[234]

i) Décision n° 2010-25 QPC du 16 septembre 2010

119. The database in issue was set up by a statute and contained the DNA of various criminal offenders.[235] The *Conseil* did not find the scheme to breach the constitutional right to privacy, but it found that the legislature struck a proportionate balance between the right to privacy and the public interest. First, it found that the scheme contained the same guarantees that are embedded in the

[232] ibid [3].
[233] *Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité du 25 octobre 2011.*
[234] 'Commentaire Décision n° 2012-652 DC du 22 mars 2012 Loi relative à la protection de l'identité' *prepared and put on line by the Conseil Constitutionel* page 14.
[235] This database was named: *Fichier national automatisé des empreintes génétiques* (FNAEG).

general Data Protection legislation (itself mirroring the requisite safeguards of the EU Directive 95/46/EC); second it found the institutional guarantees were deemed sufficient. They are mostly as follows: the database being processed and supervised by the court as opposed to the government; clear definition of the range of criminal offences that entail the processing of the criminal offenders' DNA data; efficient guarantees of clearing the database of DNA data belonging to mere suspected persons; further use of the database being strictly confined to similar law enforcement purposes. The test the *Conseil* adopted in this case amounted to a level of strict proportionality scrutiny.[236]

120. Prior to this decision, the *Conseil* issued a similar opinion in the case of a database containing the data of sexual offenders that could be consulted by public authorities in assessing applications for jobs that involve a high level of security.[237]

[236] Décision n° 2010-25 QPC du 16 septembre 2010, 14

[237] Décision n° 2004-499 DC du 29 juillet 2004 on the so called FIJAIS database

GERMANY

155

OVERVIEW

121 In Germany, no constitutional challenge has arisen specifically in relation to a biometric identification scheme.[238] However, constitutional challenges have arisen in the context of the transfer of information collected through the national population census,[239] the online searching of computers by intelligence authorities,[240] the retention of telecommunications data[241] and automatic number plate recognition.[242] These constitutional challenges have been based either on the 'right to informational self-determination' or the 'right to the integrity and confidentiality of information technology systems', which have both been implied into the German Constitution ('*Grundgesetz*'), or on the right to secrecy of communications that is contained in Article 10(1) of the German Constitution.[243]

---

[238] Note however, that a recent challenge to the storage of biometric information in RFID chips in passports (namely, the right of a person to be issued a passport without his fingerprints being taken) was made in a case before the Gelsenkirchen District Administrative Court in Germany *('Verwaltungsgericht Gelsenkirchen')*. This case (*Verwaltungsgericht Gelsenkirchen, Beschluss vom 15. Mai 2012, Aktenzeichen 17 K 3382/07*) challenged the validity of Article 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004, as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009. The question of the validity of the regulation has since been referred to the Court of Justice of the European Union ('ECJ') for determination See: InfoCuria - Caselaw of the Court of Justice, 'Reference for a preliminary ruling from the Verwaltungsgericht Gelsenkirchen (Germany) lodged on 12 June 2012 – Michael Schwarz v Stadt Bochum (Case C-291/12)' <http //curia.europa eu/juris/document/document jsf?text=&docid=126045&pageIndex=0&doclang=EN&mode =req&dir=&occ=first&part=1&cid=963296> accessed 21 February 2013. See further European Union, above para 95.

[239] BVerfG 15 December 1983, *BVerfGE* 65, 1 – *Census Act Case ('Volkszahlung')*, discussed in S Michalowski and L Woods, *German constitutional law: the protection of civil liberties* (Ashgate 1999) 120-123.

[240] German Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07, available at <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html> (in German) and at <http://www.bverfg.de/en/decisions/rs20080227_1bvr037007en.html> (in English) accessed 21 February 2013 See also BVerfG 27 February 2008, *BVerfGE* 120, 274 – *Online Computer Surveillance Case*, discussed in D Kommers and R Miller, *The Constitutional Jurisprudence of the Federal Republic of Germany* (3rd edn, Duke University Press 2012) 417

[241] German Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 2 March 2010, reference number 1 BvR 256/08, available at <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html> (in German) accessed 20 February 2013, see however German Federal Constitutional Court (*Bundesverfassungsgericht*) Press Office, 'Data retention unconstitutional in its present form' (Press Release No. 11/2010, 2 March 2010) <http://www.bverfg.de/pressemitteilungen/bvg10-011en.html> accessed 21 February 2013.

[242] German Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 11 March 2008, reference number: 1 BvR 2074/05 and 1 BvR 1254/07 <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html> (in German); see also G Hornung and C Schnabel, 'Data Protection in Germany II: Recent decisions on online searching of computers, automatic number plate recognition and data retention' (2009) 25(2) Computer Law & Security Review 115, 117-119

[243] German Constitution (*Grundgesetz*), Article 10, <http://www.bundestag.de/htdocs_e/documents/legal/index.html> (in English) accessed 21 February 2013. Note

122 In addition, Germany has one of the strictest statutory frameworks for data protection in the European Union.[244]

LEGAL FRAMEWORK

a) Constitutional protection

123. A general right to privacy is not expressly stated in the German Constitution. However, the German Federal Constitutional Court has found that it is implied by the 'right to the free development of one's personality'[245] that is contained in Articles 2(1) and 1(1) of the German Constitution.[246] Article 2(1) states that:

> [e]very person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.[247]

124. Article 2(1) has been interpreted as extending not only to a right to privacy *('Recht auf Privatsphäre')*[248] but also to a right to informational self-determination *('Recht auf informationelle Selbstbestimmung')*[249] and a right to the integrity and confidentiality of information technology systems *('Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme')*.[250] State action that restricts these rights is justified only if it has a legal basis and if it is proportional.[251] In addition, the Court has stressed that in determining the content and scope of the right in Article 2(1), the guarantee of human dignity in Article 1(1) must be taken into consideration.[252]

---

that this version of the German Constitution was translated by Professor C Tomuschat and Professor D Currie, and revised by Professor C Tomuschat and Professor D Kommers in coorperation with the Language Service of the German Federal Parliament (*Deutscher Bundestag*), and reflects the German Constitution as at October, 2010.

244 Privacy International, 'Germany Country Report' (1 January 2011) <https://www.privacyinternational.org/reports/germany> accessed 21 February 2013

245 This right is also sometimes described in English as the 'right to self-determination', or as an 'autonomous fundamental right' See T Hoeren and A Rodenhausen, 'Constitutional Rights and New Technologies in Germany' in R Leenes, B Koops and P De Hert (eds), *Constitutional Rights and New Technologies: A Comparative Study* (Asser Press c2006)

246 ibid 138.

247 German Constitution (*Grundgesetz*) (n 243), Article 2(1)

248 See BVerfG 26 April 1997, *BVerfGE* 90, 255, 260, discussed in R Leenes et al (n 245) 138-145.

249 *Census Act Case* (n 239)

250 *Online Computer Surveillance Case* (n 240)

251 R Leenes et al (n 245) 138

252 German Constitution (*Grundgesetz*), Article 10.

125 As well as these implied rights, Article 10 of the German Constitution provides that restrictions on '[t]he privacy of correspondence, posts and telecommunications' may be ordered only pursuant to a law'.[253]

b) Statutory protection

126. In Germany, data protection rights are also provided for in a number of statutory instruments. The Federal Data Protection Law *('Bundesdatenschutzgesetz', 'BDSG')*, constitutes the main and general legal framework for the protection of personal data, and implements the general EU Directive 95/46/EC.[254] Compliance with the provisions of the Federal Data Protection Law is monitored by the Federal Commissioner for Data Protection and Freedom of Information *('Bundesbeauftragter fur den Datenschutz and die Informationsfreiheit', 'BfDI')*.[255]

127. Special rules concerning specific technologies are also found in the Telecommunications Act *('Telekommunikationsgesetz', 'TKG')*[256] and the Telemedia Act *('Telemediengesetz', 'TMG')*.[257] In addition, all of Germany's 16 States *('Länder')* have their own specific data protection regulations that cover the public agencies of each state [258]

CASE LAW

a) Census Act Case

128 The Court first developed the right to informational self-determination in the *Census Act Case*.[259]

i) The nature and purpose of the challenged legislation

129. A national census was to be held according to the National Census Act (1983). The intention behind the census was to obtain comprehensive statistical data regarding the population, in particular, demographic, social and economic information on

---

[253] German Constitution (*Grundgesetz*) (n 245), Article 10.
[254] Federal Data Protection Law *('BDSG')* <http://www.gesetze-im-internet.de/bdsg_1990/> (in German and English) accessed 21 February 2013, EU Council Directive 95/46/EC (n 174); R Leenes et al (n 245) 145.
[255] Federal Commissioner for Data Protection and Freedom of Information *('BfDI')* available at <http://www.bfdi.bund.de/Vorschaltseite_DE_node.html> (in German and English) accessed 21 February 2013
[256] Telecommunications Act *('TKG')* available at <http://www.gesetze-im-internet.de/tkg_2004/> (in German) accessed 21 February 2013, Leenes ibid
[257] Telemedia Act *('TMG')* available at <http://www.gesetze-im-internet.de/tmg/> (in German) accessed 21 February 2013; Leenes ibid
[258] Leenes ibid
[259] *Census Act Case* (n 239)

which the government could base future political and economic decisions. The National Census Act placed an obligation on every household to fill in and return a census form and provided for the possibility of different state agencies comparing and exchanging the collected data.[260]

ii) The nature and scope of the right to informational self-determination

130. The court found that the general right of personality in Article 2(1), in conjunction with the guarantee of human dignity in Article 1(1), gave rise to an implied right to informational self-determination. The Court described the right to informational self-determination as follows:

> Individual self-determination, however, presupposes – even under the conditions of modern information processing techniques – that the individual has the freedom to decide whether to perform or omit actions, including the possibility of acting according to this decision. A person who cannot safely tell what information about him regarding certain areas is known to his social environment, and cannot to some extent assess the knowledge of potential partners of communication, can be essentially inhibited in his freedom to make autonomous plans and decisions. ... If someone is uncertain whether deviant behaviour will at any time be noted and as information interminably be stored, used or transmitted, he will try not to stand out by such behaviour. ... *It follows that the free development of one's personality under the modern conditions of data processing presupposes the protection of the individual against unlimited collection, storage, use and transmission of his personal data.* This protection is therefore included in the basic right of Article 2(1) in conjunction with Article 1(1) of the Constitution. The basic right guarantees insofar the right of the individual to decide in principle about the disclosure and the use of his personal data (emphasis added).[261]

131. In determining what type of information was covered by the scope of the right, the Court considered that the need for information to be protected depended not only on its content, but also on its possible use.[262]

iii) Proportionality assessment

132. The court balanced the state's need for comprehensive statistical information to enable efficient future planning against the individual's personality right and concluded:

> A possible transmission of data which are neither anonymised nor statistically prepared, i.e. data with personal reference, raises special problems. Surveys for

[260] ibid 120
[261] ibid 120-121.
[262] ibid at 122.

> statistical purposes embrace individualised information concerning the individual citizen, which is not necessary for statistical purposes but it rather only necessary for the procedure of data collection. All this information can be transmitted according to express statutory authorisations, as long as the transmission serves the purpose of its statistical preparation by another authority and as long as the requirements of the protection of the personality right, in particular the secrecy of the statistics and the commands of an early anonymisation ... are guaranteed.[263]

That is, the Court held that the collection of data in the course of a national census was in itself constitutional, as long as the data were only used for statistical purposes, and as long as they were anonymised as early as possible.

iv) Violation of the right to informational self-determination

133. However, the Court held that one provision of the National Census Act, which provided that the personal data to be given on every form could be compared with police registers to see whether the information in those registers was up-to-date, was unconstitutional. The Court held that this use of the information was an unjustified violation of the right to informational self-determination and of Article 2(1), as the information was provided for statistical purposes.[264]

b) Online Computer Surveillance Case

134. The *Online Computer Surveillance Case* is considered to be one of the most important constitutional cases on privacy issues in Germany since the *Census Act Case* in 1983.[265]

i) The nature and purpose of the challenged legislation

135 The Court considered provisions of a North-Rhine Westphalia statute that authorised intelligence authorities to access information technology systems secretly 'through the use of technical means'.[266] The statute did not set out the mode of access that could be used to conduct covert surveillance searches, nor provide for any other substantial or procedural privacy safeguards.[267]

---

[263] ibid 122
[264] ibid 122-123
[265] Privacy International (n 244), and Kommers and Miller (n 243) 417
[266] *Online Computer Surveillance Case* (n 240); G Hornung and C Schnabel (n 242) 116.
[267] ibid

ii) The nature and scope of the right to the integrity and confidentiality of information technology systems

136. The Court considered that neither the right to secrecy of telecommunications in Article 10 of the German Constitution nor the right to informational self-determination covered the online searching of information technology systems.[268] However, the Court found that this technology was protected under the Constitution by deriving a right to the integrity and confidentiality of information technology systems from the general right of personality in Article 2(1), in conjunction with the guarantee of human dignity in Article 1(1).[269] The Court observed that:

> Today's personal computers can be used for a wide variety of purposes, some for the comprehensive collection and storage of highly personal information ... corresponding to the enormous rise in the importance of personal computers for the development of the human personality.[270]

137. In describing the scope of application of this right, the Court held that:

> The fundamental right to the integrity and confidentiality of information technology systems is to be applied ... if the empowerment to encroach covers systems that, alone or in their technical networking, contain personal data of the person concerned to such a degree that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of his or her personality.[271]

iii) Proportionality assessment

138. The Court did not rule out the possibility of covert searches of computers by intelligence agencies.[272] However, the Court held that such measures may only be justified where established facts indicate that there is an imminent threat to the life, physical integrity or liberty of persons, or to the foundations of the state.[273] In addition, the Court held that covert searches must be subject to judicial oversight.[274] Furthermore, the Court held that the legal basis for such measures

---

[268] ibid
[269] *Online Computer Surveillance Case* (n 240); Kommers and Miller (n 123) 417
[270] ibid
[271] ibid
[272] ibid
[273] ibid
[274] ibid

must provide safeguards to prevent any infringements of the 'core of personal privacy'.[275]

iv) Violation of the right to the integrity and confidentiality of information technology systems

139. The Court found that the impugned provisions were incompatible with the implied right to the integrity and confidentiality of information technology systems and unconstitutional, as they did not contain any of these safeguards.[276]

c) Data Stockpiling Case

140. The *Data Stockpiling Case* concerned the largest number of related proceedings ever initiated in the German Federal Constitutional Court.[277] More than 34,000 citizens filed individual actions, supported by the German Working Group on Data Retention *('Arbeitskreis Vorratsdatenspeicherung')*.[278]

i) The nature and purpose of the challenged legislation

141. In the *Data Stockpiling Case*, the Court considered the constitutional validity of amendments to the Telecommunications Act and the Code of Criminal Procedure *('Strafprozessordnung', 'StPO')*.[279] The amendments were enacted to implement European Union Directive 2006/24/EC, which required the mass storage for six months of mobile and fixed-line telephone calls and email traffic.[280] The Directive was aimed at combatting terrorism.[281]

ii) The right to secrecy of telecommunications in Article 10(1)

142 The Court considered that the challenged amendments encroached on the area of protection of Article 10(1) of the Constitution, which guarantees the right to secrecy of telecommunications.[282]

iii) Proportionality assessment

143 In examining the issue of proportionality, the Court held that:

---

[275] G Hornung and C Schnabel (n 242) 117.
[276] *Online Computer Surveillance Case* (n 240); Kommers and Miller (n 240) 417
[277] Privacy International (n 244).
[278] ibid, see also website of the *Arbeitskreis Vorratsdatenspeicherung* (in English) available at <http://www.vorratsdatenspeicherung.de/> accessed 21 February 2013.
[279] *Data Stockpiling Case* (n 124).
[280] ibid
[281] Kommers and Miller (n 243) 417
[282] *Data Stockpiling Case* (n 124)

> In view of the particular weight of precautionary storage of telecommunications traffic data, such storage is compatible with [Article 10(1) of the Constitution] only if its formulation satisfies particular constitutional requirements. In this respect, there must be sufficiently sophisticated legislation with well-defined provisions on data security, in order to restrict the use of data, and for transparency and legal protection. . In view of the scope and the potential probative strength of the retained data gathered by such storage, data security is of great importance for the proportionality of the challenged provisions. There is a need for legislation which provides for a particularly high degree of security, whose essential provisions are at all events well-defined and legally binding.[283]

iii) Violation of the right to secrecy of telecommunications in Article 10(1)

144 The Court considered that the retention of such a vast amount of sensitive data would unnecessarily impede the exchange of communication amongst citizens, and were thus incompatible with the right to secrecy of telecommunications guaranteed in Article 10(1).[284]

145 According to the Court:

> [A]n encroachment on liberty interests of such importance ... would be compatible with Article 10(1) .. only if stockpiling were conducted by private actors for the state's use in investigating criminal acts or preventing security threats, both of which must involve considerable gravity.[285]

[283] German Federal Constitutional Court (*Bundesverfassungsgericht*) Press Office, 'Data retention unconstitutional in its present form' (Press Release No. 11/2010, 2 March 2010) <http://www.bverfg.de/pressemitteilungen/bvg10-011en.html> accessed 21 February 2013.

[284] *Data Stockpiling Case* (n 124); G Hornung and C Schnabel (n 242) 121

[285] *Data Stockpiling Case* (n 124), Kommers and Miller (n 243) 418

9.7 Operations and Ongoing maintenance

9.7.1 Support and Maintenance of Application

The objective of post implementation application maintenance is to provide application maintenance and support services, including request based services (problem requests/defect fixes), enhancements, configuration management and post release support. As part of these services, BSP should provide support for upgrade, bug fixes, enhancements, operational support, and assistance to the stakeholders.

Full-time support of programmers shall be provided to UIDAI after Acceptance of System for the contract period. The Programmer deployed at UIDAI should be able to handle any change in the application as requested by UIDAI. Vendor should propose the nature and quantity of the support.

The services include:

Bug-fixes and end-user problem resolution:

The stakeholder support would include all activities related to resolving the bugs / defects reported by the users. Every bug / defect should be logged. Every bug / defect should be categorized on the severity levels. BSP should identify the solution and take necessary approvals from the stakeholders and release the patch for User Acceptance Testing (UAT) after fixing the defects. BSP should document defects / bugs encountered as well as document the resolution of the same.

New development and enhancements

UIDAI intends to upgrade the version of the application during the contract period. If there are changes in requirements during the contract period post go-live, BSP in consultation with UIDAI is expected to define a formal process to manage the requirements changes as defined for illustration below:

BSP shall be responsible to initiate the change requests suggested by stakeholders, assess the need to implement the suggested changes, take necessary approvals to implement the suggested changes. UIDAI will forward the approved change requests to BSP.

BSP shall maintain a change request log to keep track of the change requests. Each entry in the log shall contain a Change Request Number, a brief description of the change, the effect of the change, the status of the change request, and the key dates.

BSP shall assess the effect of the change by performing impact analysis.

BSP shall maintain the change request log with updated information and provide the same to UIDAI as and when desired.

UIDAI shall be informed of all version upgrades (minor & major), patches, releases and enhancements. UIDAI will review the impact of the change and will its own discretion decide if the change should be implemented. The BSP will install, test and configure the changed solution in the test and production environment.

Configuration management and Version Control

With the objective of keeping track of the version updates in the application, BSP should adhere to the configuration management process defined in conjunction with the stakeholders. BSP may be required to assist the stakeholders in ensuring that a copy of the production environment is backed up and stored in the repository before the new / modified components are copied to Production. BSP may be required to assist the stakeholders' personnel in restoring the backed up application versions for testing purpose mainly addressing the restorability of the media.

Test management

Test management procedure should be defined in conjunction with the stakeholders to ensure smooth transition of the application changes from test environment to production environment. As part of the release management BSP should perform the following activities:

BSP should group the related change requests, assess their development progress and accordingly prepare a schedule for their release to production.

BSP should in consultation with the stakeholders prepare a detailed release plan for every release. This plan should include the release number and date of release. It should also contain details about the change request to be released.

9.7.2 Help Desk

A helpdesk is envisaged with a minimum of helpdesk personnel to be provided for the resolution of technical queries by internal users. Typical helpdesk activities shall include:

- Deployment of sufficient manpower to attend the helpdesk requests for extending technical support on solution

D R. Nanavati, DGS

L-1 Identity Solutions Operating Company Private Limited

- Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through a dedicated phone number
- Track each incident / call to resolution.
- Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed upon and developed by BSP and UIDAI.
- Coordinate with respective OEM for closure of calls.
- Analyze the incident / call statistics and provide monthly reports including but not limited to:
    - Type of incidents / calls logged
    - Incidents / calls resolved
    - Incidents / calls open.

9.7.3 Warranty and Annual Maintenance Contract (AMC) Administration

BSP should ensure availability of Warranty and Annual Maintenance Contract (AMC) support with all the OEMs for proposed software components including biometrics algorithms proposed. This Warranty and AMC support period should coincide with the entire duration of the contract. BSP should track the Warranty and AMC for all the assets at the UIDAI offices, third party locations and DC/DR sites and initiate procedure for renewal of the same at appropriate points in time.

9.7.4 MIS Reports and Incident Reporting

The following is an indicative list of MIS reports to be submitted by the BSP post go-live. The selected BSP shall also draw an exhaustive list of reports along with UIDAI. BSP shall submit the reports on a regular basis in a mutually decided format. BSP shall submit 2 hard copies and 1 soft copy of each of the reports.

1. Log of preventive / break-fix maintenance undertaken.
2. Summary of changes undertaken in all the datacenters including major changes like configuration changes, release of patches, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.
3. Consolidated SLA Report

P. Nanavati, DDG

L-1 Identity Solutions Operating Company Private Limited

4. Summary of incidents reported like Application down, Components down, overall downtime, security vulnerabilities detected, hacker attacks / security threats, peaking of utilization, etc
5. Bug / defect resolution reports including the analysis of bugs / defects resolved, pending, completion time, responsiveness, concern areas, etc.
6. Change Request Logs with their resolution status
7. Incident Reporting (as and when it occurs)
    - Complete system down – with root cause analysis
    - Peaking of resource utilization on any component
    - Bottlenecks observed in the system and the possible solutions and workarounds.
8. Security Incident Reporting (as and when it occurs)
    - Detection of security vulnerability detection with the available solutions / workarounds for fixing.
    - Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.

9.8 Technical Reports

9.8.1 ABIS Reports

ABIS reports will include technical data mentioned in Sections 6.1 and 6.2.4. UIDAI and BSP will jointly determine frequency and content of the reports. The report will include accuracy reports (FMR, FNMR, FPIR, FNIR).

9.8.2 Data Quality Monitoring & Reporting

The quality of captured data is related with accuracy of matching. It is therefore very important that the BSP should continuously monitor the data quality and publish reports, generate exceptions in case quality going below the threshold. Data quality monitoring is complementary to benchmarking, and helps to analyze and correct the problems with the capture process. The primary objective is to identify the sources of the quality problems and to implement the corrective actions. The functionality will be implemented in the analytics module using the functionality provided by Biometric SDKs.

B.B. Nanawati, DGS

L-1 Identity Solutions Operating Company Private Limited

. It is assumed that the

- Data quality of capture would be received with the image. Image would be received in raw form.
- Original captured images may be appropriately compressed using published loss-less compression algorithm for optimization of storage and transmission. The Compression will not alter the quality of image.

In summary, the BSP should provision for following scope of work related with Data quality monitoring and reporting:

- The BSP should centrally administer Image level quality checks and thresholds
- The BSP should implement a process which generates automated exception, if despite best efforts image captures do not meet quality standards. The BSP should design and implement mechanism which would provide direct feedback of quality and capture related shortfalls to registrars
- The BSP should implement a process which implements Image enhancements techniques to enhance biometric feature extraction to acceptable levels.
- The BSP should implement a process for achieving consistency across capture devices and, in the case of iris, distance from camera and lighting conditions, by applying variable image enhancement based on known issues of a specific device.
- The BSP would present the statistical data to UIDAI authority on monthly basis. This will help UIDAI to take a decision, in case threshold value needs to be adjusted based on inputs from field.
- The BSP should implement a mechanism to remote update of threshold value of capturing process in UID data capturing application. The patch should be automatically pushed when capture application connects next to UID data center for data upload.
- The BSP should implement a mechanism for automated detection of fingerprint sequence issues to detect a wrongly indexed finger or repeated finger to cause operator errors leading to fraudulent situations.
- The BSP should implement a mechanism for automated exception marking if despite best efforts image captures do not meet quality standards

D.P. Nanawati, DDG

L-1 Identity Solutions Operating Company Private Limited

Reporting

- The BSP should perform analysis of captured quality and accuracy of matching on weekly basis.
- The solution being offered by the BSP should have adequate safeguards and validations to ensure that all data relating to an applicant, together with the photograph, biometrics get tagged together and that there is no mix-up of the particulars relating to one applicant with those of others. The system should immediately capture any exception and publish a report on a weekly basis.
- The BSP should report situations where biometric features could not be captured due to various reasons, like old and infirm persons, persons with one or no hands, children, technological limitations, etc. This report should be published on weekly basis
- Weekly reports on capture statistics and quality level analysis based on registrars, location, scanner type

9.9 Training

As part of system implementation, BSP shall impart training, to staff of UIDAI and of service providers as nominated by UIDAI, on the solution related to configuration, usage, API, performance tuning and measurement and Technical reports as indicated in the Terms of Reference. The Training program shall involve both in-class and online training sessions. The BSP shall develop the required training materials. Main tasks include:

a. Estimating timeframe for overall training program

b. Designing Curriculum & develop training materials

d. Delivering classroom training

e. BSP shall training curriculum that shall include at least the list of course as mentioned in the below:

1. ABIS System Configuration and Administration (including backup)
2. SDK Tool Kit – development, Configuration and Integration
3. ABIS quality and accuracy management
4. Input Data Quality Monitoring
5. Performance Measurement

S.P. Nanavati, DEC

L-1 Identity Solutions Operating Company Private Limited

6. Benchmarking

9.10 Project Management Procedures

The BSP is required to adopt a comprehensive and effective project management methodology together with efficient and reliable tools.

The BSP would prepare a detailed and comprehensive *Project Plan* that shall address at the minimum the following:

- Define an organized set of activities for the project and identify the interdependencies between them.
- Establish and measure resource assignments and responsibilities.
- Construct a project plan schedule with milestones.
- Measure project deadlines, budget figures, and performance objectives.
- The Plan document shall include:
    - Project Organization and Management plan
    - Software Design and customization plan
    - Implementation plan
    - Pre-commissioning, Operational and User Acceptance Testing Plan
    - Design, Delivery and Installation Plan for Servers and Storage
    - Training Plan
    - Resource planning and loading for each phase/activity. This must also indicate where each resource would be based during that phase, i.e., onsite at UIDAI's offices or at the BSP premises.
    - Technical Support Plan
    - Quality Plan with Quality Assurance and Control Process details which must include (but not limited to) detailing on Metrics, Reviews, Problem Reporting and Corrective action etc.
    - Technical and Operational Process which must include (but not limited to) detailing on Methods, Tools, Techniques etc.
    - Contingency Plan document containing emergency response procedures; backup arrangements, procedures, and responsibilities; and post-disaster

J.D. Nanawati, DDG

L-1 Identity Solutions Operating Company Private Limited

recovery plans, procedures and responsibilities in compliance with the BCP plan of UIDAI

- Communicate the project plan to stakeholders with meaningful reports.
- During the project implementation the BSP shall report to UIDAI, on following items:
  - Results accomplished during the period (fortnightly).
  - Cumulative deviations to date from the schedule as specified in the finalized Project Plan.
  - Corrective actions to be taken to return to planned schedule of progress.
  - Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of the BSP.
  - Other issues and outstanding problems, and actions proposed to be taken.
- Progress reports on a fortnightly basis.
- Identify the activities that require the participation of UIDAI and communicate their time requirements and schedule early enough to ensure their full participation at the required time.

The Project plan prepared by the BSP would be reviewed by UIDAI.

The BSP would update and maintain the Project Plan throughout the duration of the engagement. All changes are to be reviewed and approved by UIDAI.

Project Documentation and Manuals

The BSP shall create and maintain all project documents that would be passed on to UIDAI as deliverables as per the agreed project timelines. The documents created by the BSP will be reviewed and approved by the UIDAI. UIDAI would also approve any changes required to these documents during the course of the project.

The project documents include but are not limited to the following:

- Inception Report containing the Detailed project plan
- All Test Plans. Test Cases, Test Input data set and Test Results
- Training and Knowledge Transfer Plans

L-1 Identity Solutions Operating Company Private Limited

- Detailed Hardware Specifications and related hardware configuration document
- Roll Out Completion Report
- SLA and Performance Monitoring Plan
- Issue Logs

The BSP shall submit a list of deliverables that they would submit based on the methodology they propose. The BSP shall prepare the formats/templates for each of the deliverables upfront based upon industry standards and the same will be approved by UIDAI prior to its use for deliverables.

All methodology and documentation shall conform to the standards like CMM/CMMi, wherever applicable. All project documents are to be kept up-to-date during the course of the project.

Application Manuals

The BSP would prepare the necessary manuals for ABIS and SDK and training materials including (but not necessarily limited to):

- Technical/Operations manual for applications in English.
- User manuals for application in English.

The BSP shall maintain a log of the internal review of all the deliverables submitted. The logs shall be submitted to UIDAI on request.

All project documentation shall conform to the highest standards of software engineering documentation.

All the manuals and training materials will be provided to UIDAI as two sets of hardcopies and two sets of softcopies on separate CDs.

9.11 Migration of solution to other facility

BSP shall UIDAI and UIDAI nominated third party representatives in transfer of solution and infrastructure to another datacenter facility during the contract period. BSP, on prior notice from UIDAI, shall deploy required personnel to support the migration of the infrastructure and in setting up installation, configuration and commissioning of the solution at the new facility till the time the solution is operating to the expectations of the UIDAI

R.S. Manavati, DDG

L-1 Identity Solutions Operating Company Private Limited

10 ACCEPTANCE OF SOLUTION

Acceptance schedules, detailed acceptance tests, formats for acceptance reports and dissemination mechanism for such reports shall be drawn by the BSP in consultation with UIDAI.

The Acceptance of the solution shall be provided by the UIDAI only after the following conditions have been met successfully to the satisfaction of the purchaser.

1. Successful go-live of the Biometric solution to Primary site and to BCP site to the extent necessary for meeting the desired objectives.
2. Successful operation for 30 working days after complete rollout of the system meeting the Services Level Agreement as agreed between UIDAI and BSP at the time of signing of contract.
3. Completion of all the documentation required as part of this RFP and as desired by the purchaser to the satisfaction of the UIDAI.
4. Installation and Configuration of all the components of the solutions including hardware, software, Storage, accessories to the satisfaction of UIDAI at both the sites and successful testing of all components.
5. The Biometric Solution Providers should demonstrate the performance of the application in "live" condition at BCP site to the satisfaction of UIDAI within a timeframe of three months from the date of successful go-live from the Primary site

The following is the indicative acceptance criteria for some of the deliverables and work products

Acceptance criteria for Biometric Solutions

1. Successful testing / re-testing of all the application test cases
2. Adherence to the acceptance test cases developed for each requirement of Biometric Solution Component as stated in Annexure . Minimum Requirements and Technical Particulars
3. Review and acceptance of all the application deliverables including documentation
4. Successful adherence to SLAs on SLA testing/measurement undertaken

D. P. Nanavati, DSG

L-1 Identity Solutions Operating Company Private Limited

5. Successful execution of the application related training to all identified users
6. Successful go-live and closure of all incidents of the solution

Acceptance criteria for Documented Work Products/ Deliverables

1. Finalization of expected contents of work product with UIDAI prior to submission of draft document
2. Submission of draft document for UIDAI's review after sufficient internal review by the BSP
3. Closure of review comments from UIDAI within the timelines stated
4. Acceptance of revised draft(s) by UIDAI based on adequacy and quality of the final submission

11 CONSTITUTION OF TEAM

The professional staff proposed for this project by the bidder will play a key role in successful rollout of the biometric solution and the following indicative profiles are required to be provided by the bidder. Should any additional profiles be suggested by the bidder, the role of the profile shall be clearly outlined and the Lifecycle Deliverables to which the profile will contribute shall be clearly defined.

The key staff will be organized as follows

Project Organization	Role	Involvement
Project In-charge	Manages the overall project, resources and deliverables. Coordinates with R&D and support organizations of the BSP.	Full time: From signing of contract until 10M enrolment Part time: After 10M
Integration Engineer (2 personnel)	Provides support for integration and develops necessary tools for ABIS and SDK to fully integrate with UID application.	Full time: From signing of contract until acceptance testing of ABIS and SDK (with Verification and monitoring integration)
Biometric Specialist (2 personnel)	Evaluates biometric data, configures biometric	Full time: From signing of contract until acceptance testing

Project Organization	Role	Involvement
	algorithms, computes performance and accuracy numbers and provides recommendation on optimum configuration of the solution.	Part time: until the solution crosses 10M size
System Performance Specialist	Configures the solution for UIDAI to support requirements. Tunes the system as load and needs changes. Estimates hardware and other infrastructure requirements.	Full time: From signing of contract until acceptance testing Part time: until the solution crosses 10M size
Q&A and Test Engineer	Designs the test and conducts final unit and system testing of the entire solution to meet stated targets	Full time: From the signing of the contract until acceptance

The above organization does not show personnel required for on-going installation, maintenance and support of the solution including hardware.

Following are the detailed descriptions of the expectations from the profiles.

11.1 Project In-charge

11.1.1 Role

- Manages the overall project, resources and deliverables.
- Coordinates with R&D and support organizations of the BSP.
- Coordinates all technical activities with the UID stakeholders
- Provides periodic status reports to the PMC

11.1.2 Qualification & Experience

- Should have over 10 years of experience in software/biometric project/product implementation
- Should have at least four years experience in software project implementation
- Should have advanced degrees in engineering/computer sciences/information technology

- Should have led a biometric project of comparable size and complexity (10M DB or multi-modal ABIS)

11.2 Integration Engineer

11.2.1 Role

- Provides support for integration of ABIS and SDK.
- Analyzes interoperability issues
- Develops necessary tools to fully integrate with UID application.
- Coordinates with R&D and support organizations of the BSP.
- Works closely with ASDMSA and UIDAI technology team to design the integration
- Helps develop test cases and criteria

11.2.2 Qualification & Experience

- Should have over 7 years of experience in software project/product integration
- Should have at least four years experience in software integration of biometric applications using similar architecture
- Should have been a lead integration engineer for a biometric project of comparable size and complexity (10M DB or multi-modal ABIS)
- Should have advanced degrees in engineering/computer sciences/information technology
- Should have thorough knowledge of Linux, middleware, high performance messaging, Java/J2EE, C, ISO standards for biometrics and other technologies needed for server integration or
- Should have thorough knowledge of Windows, .NET, C#, C, biometric device protocols and formats.

BSP shall provide at least 2 personnel for the above role.

11.3 Biometric Specialist

11.3.1 Role

- Evaluates biometric data quality and analyzes corresponding quality issues
- Configures biometric algorithms
- Trains the biometric solution
- Conducts performance and accuracy experiments

D. R. Nanaweti, pps

L-1 Identity Solutions Operating Company Private Limited

- Computes performance and accuracy numbers and
- Provides recommendation on optimum configuration of the solution.

11.3.2 Qualification & Experience

- Should have over 7 years of experience in biometric solution implementation
- Should have been a lead biometric specialist for a project of comparable size and complexity (10M DB or multi-modal ABIS)
- Should have good knowledge of application level biometric integration
- Should have advanced degrees in engineering/computer sciences/information technology with emphasis on biometric (or computer vision)
- Should have thorough knowledge biometric algorithms, biometric devices and identity management systems.
- Should have over 2 years of experience in conducting performance and accuracy experiments
- Should have over 2 years of experience with iris devices and algorithm (1 specialist)

BSP shall provide at least 2 personnel for the above role.

11.4 System Performance Specialist

11.4.1 Role

- Optimizes performance of the ABIS through system level configuration and tuning
- Configures the solution for UIDAI to support requirements.
- Estimates hardware and other infrastructure requirements.
- Should be able to assist in the day-to-day tasks, including, but not limited to, monitoring of system activities, analysis of system utilization and resources, capacity control, performance tuning, coordination of system upgrades or fixes, and generating reports as required.

11.4.2 Qualification & Experience

- Should provide highly specialized technical expertise to handle System Administration challenges for systems of size and complexity that are being proposed as part of this solution.
- Should have over 7 years of experience in system administration and system performance

P.B. Nanavati, BDS

L-1 Identity Solutions Operating Company Private Limited

- Should have been a lead system performance specialist for a project of comparable size and complexity (biometric, high performance middleware, Linux, COTS H/W, high availability)
- Should have good knowledge of biometric systems
- Should have degree in engineering/computer sciences/information technology

11.5 Quality Assurance (QA) & Test Engineer

11.5.1 Role

- Leads QA & test integration teams through all phases of QA activities
- Responsible for designing and conducting integration test for ABIS and SDK
- Implements automation using a variety of automation technologies.

11.5.2 Qualification & Experience

- Should have over 7 years of experience in QA/Test
- Should have been a lead QA engineer for a project of comparable size and complexity (biometric, high performance middleware, Linux, Java/J2EE, .NET)
- Should have good knowledge of application level biometric integration
- Should have degree in engineering/computer sciences/information technology
- Should have previous experience using automation test technologies

B. P. Nanavati, DDG

L-1 Identity Solutions Operating Company Private Limited

12 PROJECT PLAN & TIMELINES

The project shall commence with the preparation and deployment of the solution in the form of Proof of Concept (PoC) that shall cater to the early enrolments of the residents. The solution initially may not be a fully tested and tuned solution as is expected for the subsequent stages of the project, but should however at minimum, be able to integrate with UID application and meet the performance expectations as stated in Clause 9.2 Implementation of Solution as Proof of Concept.

The BSP shall simultaneously initiate the supply, installation and configuration of the hardware for the solution to cater to 1 Crore enrolments. On completion of the same, the acceptance testing on the solution shall be undertaken based on enrolments already undertaken by the solution. While the solution is formally accepted, it shall be tuned continuously till the time first 1 Crore enrolments are reached or till completion of 12 weeks after acceptance, whichever is earlier. On attaining this milestone, the measurement of SLA shall be undertaken by UIDAI and the solution shall commence formal adherence to the Service Level Agreement for Solution related performance levels as stated in Attachment – Draft Service Level Agreement whereby the BSP shall submit a formal undertaking on SLA compliance. The dynamic allocation shall commence from with the activation of Solution related SLAs as per the rules stated in **Annexure D – Work Allocation & Service Levels**

BSP is expected to follow the schedule as mentioned below. The BSP shall ensure that the Milestones are attained and are accepted by UIDAI as per schedule mentioned in the table below post review.

T is the Date of award of Contract

S. N.	Milestone	Time for Completion
1.	a. Mobilization of Team b. Commencement of supply of hardware for 1 Crore enrolment c. Conduct a kick-off meeting with UIDAI with participation from key personnel proposed for the project to discuss the project plan for way forward d. Submission of plan for procurement, transportation, installation and commissioning of hardware in pilot data center e. Co-ordinate with Data Center service provider and prepare a blue print for deployment of hardware, ensure availability of power and other environmental facilities in the datacenter f. Set up the required Test and Production environment s for the rollout of PoC. The hardware used for Solution Demonstration exercise as part of the RFP evaluation process could be used for the rollout of PoC, if found adequate to meet the requirements based on expected enrolment transactions. g. Begin to supply SDK perpetual licenses of the proposed multimodal SDK to cater to requirements as stated in Clause 4 of this section h. Support ASDMSA in developing the client enrolment software through provisioning licensing, training and services. SDK licenses must not use hardware license key or keyed to ID (such as CPU, serial number, Ethernet ID).	T + 1 Week
2.	a. Setup of Test and Production Environment with a view to start the Proof of Concept for Biometric Solution b. SDK integration with client enrolment software	T+ 1 Week

S. N.	Milestone	Time for Completion
3.	Go-live of solution as Proof of Concept	T+2 Weeks
4.	**Go-live for 1 Crore enrolment** Activities leading to go-live shall include: a Installation, commissioning and Configuration of the hardware for the 1 Crore enrolments b Setup of Test and Production Environment with a view to start the Biometric Solution for 1 Crore enrolment c. Installation, commissioning and configuration of Biometric Solution in Test Environment d. System & Integration Testing of the Solution e. Installation, commissioning and Configuration of Biometric Solution on hardware for 1 Crore enrolment in production environment (which is provisioned by the BSP) f SDK API implementation g SDK based verification (joint task of ASDMSA & BSP) h SDK based adjudication workstation (assistance by BSP) i. SDK based monitoring and analysis functional (assistance by BSP) j. **Acceptance of the Solution**	T + 12 Weeks
5.	Commencement of adherence with SLA (Solution related SLA Activation)	T + 24 Weeks (G)
6.	Overall Solution Warranty -Warranty shall cover Software Patch update, upgrades, bug fixing and resolution of hardware and storage issues, backup.	G + 6 Months from Solution related SLA Activation

13 List of Deliverables

Sr. No.	Deliverables	Details
1.	Project Inception Report	Detailed project plan for design and implementation of solution covering all activities and related work products
2.	User Acceptance Testing Report	Unit and Integration Testing Plan and Procedure
		Testing report with fail / pass results and plan to fix the defects
		Unit and Integration Testing Completion Report
3.	Application Manuals	• Technical/Operations manual for applications in English. • User manuals for application in English
4.	Training Deliverables	Training material, manuals and completion report

Sr. No.	Deliverables	Details
5.	Undertaking for SLA Compliance	BSP shall submit a formal Undertaking on compliance with SLA after go-live as per the timelines stated in Clause 12 of this section
6.	Acceptance of Solution	Final Acceptance of Fullscale Solution after go-live as per the timelines stated in Clause 12 of this section
7.	Quarterly Deliverables	1. Consolidated SLA Compliance Report 2. Log of preventive / break-fix maintenance undertaken. 3. Summary of changes undertaken in all the datacenters including major changes like configuration changes, release of patches, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc. 4. Summary of incidents reported like Application down, Components down, overall downtime, security vulnerabilities detected, hacker attacks / security threats, peaking of utilization, etc 5. Bug / defect resolution reports including the analysis of bugs / defects resolved, pending, completion time, responsiveness, concern areas, etc. 6 Change Request Logs with their resolution status 7. Incident Reporting (as and when it occurs)

Sr. No.	Deliverables	Details
		o Complete system down – with root cause analysis o Peaking of resource utilization on any component o Bottlenecks observed in the system and the possible solutions and workarounds. 8. Security Incident Reporting (as and when it occurs) o Detection of security vulnerability detection with the available solutions / workarounds for fixing. o Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems
8.	Technical Reports	Input Data Quality report to be submitted at the end of every week and as a consolidated report at the end of every quarter both starting 2nd Quarter.

Annexure F
Minimum Requiremnets

RFP Name	Implementation of Biometric Solution
RFP No.	D-11018/14/Tech/10-UIDAI

D.P. Nanavati, ADG

L-1 Identity Solutions Operating Company (Private) Limited

Bid No. D-11018/14/Tech/10-UIDAI Annexure F - Minimum Requirements and Technical Particulars

Table of Contents

Reference	Description
VI (a)	**Minimum Requirements**
Annexure VI.a.1	ABIS Requirements
Annexure VI.a.2	SDK Requirements
	Guidance
Annexure VI.a.3	Nature of Requirements
Annexure VI.a.4	Requirements Levels
	Technical Particulars
	Overview
VI.b	**Hardware & Storage**
VI.c	**Softwares**

Private Limited * L-1 Identity Solutions Operating Company

Component Name	ABIS

Requirement ID	Requirement Description	Importance of Requirement	Scope of Work Reference
ABIS 001	How will your solution handle change in policies listed?	Level 2	5
ABIS 002	Is entire ABIS COTS? What is the version? Provide version history of last 2 years If components are not COTS, please list specific components.	Level 1	6 2
ABIS 003	Will the demographic data be used and how? Can you handle the policy of using or not using the demographic data?	Level 2	6 2
ABIS 004	If duplicates are introduced into your database, would it adversely affect your performance in any way?	Level 2	6 2
ABIS 005	What is the average time taken by your ABIS system to verify (1:1) a query against a reference database? Use your proposed hardware configuration.	Level 1	7
ABIS 006	How do you accommodate continuous improvement and performance as the database size grows? What is your approach?	Level 1	7
ABIS 007	What is the average time taken by your ABIS system to de-duplicate a query against a reference database of 10 million records? Use your proposed hardware configuration	Level 1	7
ABIS. 008	What is the average time taken to create a template from face, fingerprint and iris images (for all template types supported)? Specify your reference hardware configuration	Level 1	7
ABIS 009	How do you propose to monitor the performance (accuracies, throughput rates) of your system? Provide the details of the parameters that you measure and log.	Level 2	7
ABIS 010	The ABIS shall have ability to load balance across servers	Level 1	6 1.1
ABIS 011	The ABIS shall have ability to utilize dynamically increased CPU, RAM and storage	Level 1	6 1.1
ABIS 012	Is your system tolerant to removal/failure of server/blade?	Level 1	6.1.1
ABIS 013	The ABIS shall have ability to add nodes dynamically without bringing the ABIS down	Level 1	6 1.1
ABIS 014	The ABIS should not have a single point of failure and inherent design bottlenecks that stops it from scaling	Level 1	6 1 1
ABIS 015	The ABIS shall have ability to utilize network bandwidth provided through multiple interfaces	Level 3	6.1 1
ABIS 016	The ABIS shall have ability to scale dynamically within a server depending upon the load	Level 3	6.1 1
ABIS 017	Ability to run services in virtualized environments	Level 1	6 1 10
ABIS 018	Does your system support the use of a private cloud?	Level 2	6.1 10
ABIS 019	throttling of cpu, network and storage utilization	Level 2	6 1 10
ABIS 020	role based administration	Level 2	6 1 11
ABIS 021	automation of administrative tasks	Level 3	6 1 11
ABIS 022	ability to administer the solution with minimal user intervention with well defined user interfaces and access policies	Level 3	6 1 11
ABIS 023	a mechanism to configure the logging level for different modules	Level 1	6 1 12
ABIS 024	a mechanism to generate reports on various performance indicators	Level 1	6 1 12
ABIS 025	a mechanism to integrate with external reporting tools	Level 1	6 1.12
ABIS 026	a mechanism to search through the logs with different filters	Level 3	6 1 12
ABIS. 027	a mechanism to rotate the logs based on polices	Level 3	6 1.12
ABIS 028	work in heterogeneous storage environments with data partitioned across servers	Level 1	6.1.13
ABIS. 029	access only the data to which it was given access	Level 1	6.1.13
ABIS 030	functions with storage getting provisioned using heterogeneous storage technologies like NAS/SAN/DAS	Level 2	6 1.13

P. Nanavati, DDG

L-1 Identity Solutions Operating Company Private Limited

ABIS 031	support data partitioned across different servers	Level 2	6 1 13
ABIS 032	capability to backup and restore the data generated in the solution	Level 1	6 1 14
ABIS. 033	ability to backup of the data generated in the solution while continuing to process service requests	Level 1	6 1 14
ABIS 034	proper functioning after a restore operation	Level 2	6.1 14
ABIS 035	allowance for incremental/differential/full backup methods	Level 2	6.1 14
ABIS 036	All persistent personal information encrypted	Level 1	6 1 2
ABIS 037	communication with only the UID application.	Level 1	6.1 2
ABIS 038	Data access by authorized users only	Level 1	6 1 2
ABIS 039	Use of secure communication protocols while communicating with external components	Level 1	6 1 2
ABIS 040	security based on Access Control Lists	Level 2	6 1 2
ABIS. 041	Management functions secured (in particular CLEAR & SHUTDOWN)	Level 2	6 1 2
ABIS 042	running services without super user privileges	Level 3	6 1 2
ABIS. 043	Ability to periodically change the encryption schemes dynamically	Level 3	6 1 2
ABIS 044	re-factor/replace individual services without bringing the whole system down	Level 1	6 1 3
ABIS 045	command line based interface for configuration and management	Level 2	6 1 3
ABIS 046	automated integration from external management products such as systems management, network management, and other tools	Level 2	6 1 3
ABIS 047	the specified open standard protocol based communication	Level 2	6 1 3
ABIS. 048	ability to bring its services up and down	Level 1	6 1 4
ABIS 049	monitoring its cpu/network/storage utilization	Level 1	6 1 4
ABIS 050	continuous availability of its services even during regular management activities	Level 1	6 1 4
ABIS 051	monitoring the response time of individual services	Level 2	6.1 4
ABIS 052	Provide expected percentage of automated identification vs manual adjudication rate	Level 2	6 1 4
ABIS. 053	integration with technologies that provide data replication to have data high availability	Level 3	6 1 5
ABIS 054	functionally backward compatible	Level 2	6 1 6
ABIS 055	reverting back to original configuration in case of an upgrade failure	Level 2	6 1 6
ABIS 056	upgrading using third party software delivery systems	Level 3	6 1 6
ABIS 057	reverting back to old configuration after a successful upgrade	Level 3	6.1.6
ABIS 058	Installation - Is there install script?	Level 1	6 1 7
ABIS 059	installation and configuration without super user privileges	Level 2	6 1 7
ABIS 060	Installation – Configuration across servers through script? Dynamic?	Level 2	6 1 7
ABIS 061	How does your system handle poor quality Fingerprint, Iris and Face images?	Level 1	6 2.1
ABIS 062	What fusion mechanism do you use to combine the different modalities? What level of fusion do you propose to use?	Level 1	6 2 1
ABIS 063	Do you have prior experience in fusion of fingerprint and iris biometrics? List the deployed systems and your specific role in their implementation. What were the volumes handled by each?	Level 1	6 2 1
ABIS 064	How does your system handle records with missing or incomplete biometric data or extraneous digits in a hand?	Level 2	6 2 1

R.S. Nanavati, DDG

L-1 Identity Solutions (I) Private Limited

ABIS 065	The operation of the system will be continually monitored for the recognition accuracy (in terms of operational false positive/false negative identification rates) Should there be accuracy degradation, what will be your response?	Level 2	6 2.1
ABIS 066	Will the demographic data be used and how? Can you handle the policy of using or not using the demographic data?	Level 2	6 2.1
ABIS 067	Will the face data be used and how? Can you handle the policy of using or not using the face?	Level 2	6 2.1
ABIS 068	How will ABIS handle de-duplication of record with missing all FP and iris?	Level 2	6 2 1
ABIS 069	If multi-stage filtering is used for any modality, is it automatic/adaptive? What is the strategy used? How do you configure it? How often?	Level 2	6 2.1
ABIS 070	If you use filtering, how are the intermediate selection criteria and thresholds determined?	Level 2	6 2 1
ABIS 071	How is filtering mechanism dependent on biometric data quality, and database size?	Level 2	6 2.1
ABIS 072	How will ABIS handle de-duplication of record with missing all three biometric modalities?	Level 3	6 2.1
ABIS. 073	UID Biometric API support -- Overall compatibility	Level 1	6 2 1 1
ABIS 074	Does your fingerprint matching algorithm accommodate rotation? What are the planned constraints?	Level 1	6 2.1.1
ABIS 075	UID Biometric API support -- Identify & provide scaled score	Level 1	6 2.1 1
ABIS 076	UID Biometric API support -- Identify Against entire DB	Level 1	6 2.1 1
ABIS 077	UID Biometric API support – Identify General	Level 1	6 2 1 1
ABIS 078	UID Biometric API support – Identify provide candidate list	Level 1	6 2.1 1
ABIS 079	UID Biometric API support – Insert	Level 1	6 2 1 1
ABIS 080	Describe Candidate list selection process in ABIS (detailed flow chart)	Level 1	6 2.1.1
ABIS 081	Can the system make use of the operator segmentation of slap fingerprints?	Level 2	6 2.1.1
ABIS 082	UID Biometric API support -- Identify against subset of DB	Level 2	6.2 1 1
ABIS 083	UID Biometric API support – Identify list of IDs	Level 2	6 2 1 1
ABIS 084	UID Biometric API support – Delete	Level 2	6 2 1 1
ABIS 085	Would your system be able to match Juvenile FP with adult fingerprints of the same individual? How?	Level 2	6 2 1 1
ABIS 086	How will you support 100% feature extraction? For each modality?	Level 2	6 2 1 1
ABIS 087	There may be multiple views of the biometric data within the same record How will the ABIS take advantage of the extra information?	Level 2	6 2 1 1
ABIS 088	Fused score should be normalized. How do you convert fused score into probability of false positive identification?	Level 2	6.2 1 1
ABIS 089	Is iris sequence used or relied upon in identification?	Level 2	6.2 1 1
ABIS 090	Is the algorithm rotation invariant? If not, how is rotation handled? Is the allowed rotation configurable and what is the impact on speed/accuracy?	Level 2	6 2 1 1
ABIS 091	How do you handle the case where there are only some of the biometric position/modalities within the record match, but not the others? For example, if the ABIS does selection on the iris first, and the iris data does not match, the record will not be retrieved, even if some fingerprints match very well Please cover the worst case example(s) similar to this, specific to your ABIS	Level 2	6 2.1.1
ABIS 092	In the case that there are missing fingers, extra fingers or hand abnormalities, the identification should not rely on the sequence of the fingers Similarly, if the eye is missing, the identification should not rely on whether this is the left or right eye. How is this handled?	Level 2	6.2 1.1
ABIS 093	Can your FP segmentation algorithm make use of manually segmented coordinates if your segmentation fails when during INSERT?	Level 2	6 2 1 1
ABIS 094	Do you propose to use facial images in deduplication?	Level 3	6 2.1.1
ABIS 095	How will you support 100% segmentation?	Level 3	6 2 1 1
ABIS 096	Do you recommend UID to use black-list and/or white-list in de-duplication? What would be the purpose of the list – is it for efficiency purposes or matching with a different target FPIR?	Level 3	6 2 1 1

E.P. Nanavati, DDG

L-1 Identity Solutions

ABIS 097	Does your identification internally rely on the finger rotation angle provided by the internal segmentation algorithm?	Level 3	6.2.1 1
ABIS 098	If only one biometric sample, for example one finger, within the query record has a very high degree of similarity with the corresponding sample in a database record, but the other samples in this pair of records are not similar at all, is it guaranteed that such record will be retrieved as a candidate? Explain why	Level 3	6 2 1 1
ABIS 099	Some fingers have higher probability of sequence errors than others Is this taken into account? How?	Level 3	6 2.1.1
ABIS. 100	Is 100% of reference DB searched for each modality?	Level 3	6.2.1 1
ABIS 101	Does your solution have features to support auto correction of fingerprint sequence errors, hand inversion during segmentation?	Level 3	6 2 1 1
ABIS. 102	UID Biometric API support – Configure	Level 1	6 2.1 2
ABIS 103	UID Biometric API support – Discover	Level 1	6.2.1 2
ABIS 104	UID Biometric API support -- Ping	Level 1	6 2.1.2
ABIS 105	UID Biometric API support -- Shutdown	Level 1	6 2.1.2
ABIS 106	UID Biometric API support – Clear	Level 2	6.2.1.2
ABIS 107	UID Biometric API support – Identify against single ID (verify)	Level 1	6 2.1 3

S. P. Nanavati, DDG

L-1 Identity Solutions Operating Company Private Limited

ABIS 108	UID Biometric API support -- Identify against single ID (verify) using ISO template vendor independent section only	Level 1	6.2.1.3
ABIS. 109	Reference Database Can it export data in open (externally defined) standards format?	Level 2	6 2 2
ABIS. 110	Reference Database use Nature of DBMS proposed	Level 3	6 2 2
ABIS. 111	Does your system provide all the logs, specified in the RFP and those needed for a complete audit trail?	Level 1	6 2.3
ABIS. 112	System usage reports (CPU usage, memory usage, IO usage)	Level 2	6 2.3.1
ABIS. 113	Activity log	Level 1	6 2.3.3
ABIS. 114	List available Audit log	Level 1	6 2 3.3
ABIS 115	Change log	Level 1	6 2 3.3
ABIS 116	Log changes to database records, including deletion of records	Level 1	6 2 3.3
ABIS 117	Error log	Level 1	6.2 3.3
ABIS. 118	System availability reports	Level 1	6 2 3.3
ABIS. 119	Periodic (such as hourly) statistics on various databases including size	Level 2	6 2 3 3
ABIS 120	Information on user (operator/manager/supervisor/auditor) roles and/or privileges, including creation/deletion of users and changes to roles	Level 2	6 2 3 3
ABIS 121	Can the system do hot upgrades of minor version changes of the ABIS system?	Level 1	6 2.4
ABIS 122	How do you guarantee 99% ABIS uptime?	Level 1	6 2 4
ABIS 123	Does your system architecture have a single point of failure?	Level 1	6 2 4
ABIS. 124	Does your system support backup/maintenance without application downtime?	Level 1	6 2.4
ABIS. 125	ABIS -- Verify should remain up 99 9%	Level 1	6 2.4
ABIS 126	ABIS (excluding verify) should remain up 99%	Level 1	6 2.4
ABIS 127	Can the system do hot upgrades of major version changes of the ABIS system?	Level 2	6 2.4
ABIS 128	Can your system do dynamic reallocation of tasks to balance the load in case of addition/removal/failure/allotment of hardware?	Level 2	6 2.4
ABIS 129	Can your system support OS upgrade without interruption to services?	Level 2	6 2.4
ABIS 130	Can your system support software (such as DBMS) upgrade without interruption to services?	Level 2	6 2.4
ABIS 131	Do you need to access to any resource on the network other than the UID Application?	Level 1	6 2 5
ABIS 132	What are the authentication mechanisms for management functions?	Level 1	6.2.5
ABIS 133	What is the mechanism to secure your database? Do you support encryption?	Level 1	6 2 5
ABIS 134	ABIS will not have access and should not try to access any network resources except the resources referenced by the URLs provided through the API	Level 1	6 2 5
ABIS 135	List available Access log (including physical access of biometric servers)	Level 1	6.2 5
ABIS. 136	auditing all access and modifications (by any user) to biometric data and make these audit trails available. Audit trail should be stored	Level 1	6.2.5
ABIS 137	All backup data shall be stored in encrypted format using a key(s) available to the UIDAI.	Level 2	6 2 5
ABIS. 138	Are there any provisions to detect intentional fraud in the biometric capture process?	Level 3	

Property Private Limited 6.2.5.1 Identity Solutions

ABIS 139	Are all management, installation, configuration and administration functions available through GUI?	Level 3	6.2 6
ABIS 140	All administration and configuration functions should be available through graphical UI (in addition to command level access)	Level 3	6.2 6
ABIS 141	Does your hardware and software platforms confirm to the RFP specifications? What are the hardware and software (OS) platforms that you propose to use?	Level 1	6 2.7
ABIS. 142	ABIS should Linux OS with both 32 and 64 bit support on X86 COTS H/W	Level 1	6 2 7
ABIS 143	Is your matching algorithm specifically tuned to any particular processor?	Level 2	6.2.7
ABIS 144	Ability of the speed to be independent of specific brand of processor (CPU)	Level 3	6 2 7
ABIS. 145	Can the fingerprint verification system accept ISO 19794-2 queries?	Level 1	6 2 8
ABIS 146	FP template should be stored in reference DB in UID standards format	Level 3	6 2 8
ABIS 147	How will you support changes/upgrades in the biometric data format standards? Will you convert reference DB? Will you provide support for multiple formats by tagging?	Level 3	6 2 8
ABIS 148	How will you support standard update to templates, in particular finger print minutiae format?	Level 3	6.2 8

P. Nanavati, DDG

L-1 Identity Solutions

Annexure VI.a.2

Component Name	*Multimodal SDK*

Requirement ID	Requirement Description	Importance of Requirement	Scope of Work Refrences
SDK 001	Does your SDK provide feedback on Segmentation and Feature extraction failures for each of three modalities? Does it provide any reasons for the failures?	Level 1	6 3
SDK 002	What is the size of the average face, iris and fingerprint (proprietary and ISO/IEC 19794-2) templates?	Level 3	6.3
SDK 003	What is the average time taken by your SDK to match a pair of face, fingerprint or ins templates (for all template types supported)? Specify your reference hardware configuration.	Level 1	7
SDK 004	What is the average time taken by your SDK to create a template from face, fingerprint and iris images (for all template types supported)? Specify your reference hardware configuration.	Level 1	7
SDK 005	What is the average time taken by your FP SDK to identify a record against a reference database of 10,000 records? Specify your reference hardware configuration	Level 2	7
SDK 006	Does your FP SDK handle missing digits?	Level 1	6 3 1
SDK 007	Able to do sequence check for 2 finger device How does reliability compare to 4-4-2 sequence check?	Level 1	6 3 1
SDK 008	Does your FP SDK support 1 few identification?	Level 1	6 3 1
SDK 009	Can your FP SDK make use of manually segmented coordinates if your segmentation fails when used for Authentication server verification, manual check or analytics modules?	Level 1	6 3 1
SDK 010	Does your FP SDK support sequence checking?	Level 1	6 3 1
SDK 011	Can your FP SDK handle 2, 3, and 4 finger slap images? With missing fingers?	Level 1	6 3 1
SDK 012	What actionable feedback can your fingerprint SDK provide during the acquisition process? Please list	Level 1	6 3 1
SDK 013	Can your FP SDK handle rotated fingerprints? What is the range of rotation that you can handle?	Level 2	6 3.1
SDK 014	Able to do sequence check for 3 finger device How does reliability compare to 4-4-2 sequence check?	Level 3	6 3 1
SDK 015	Does your IRIS SDK accommodate missing iris? How does the quality check deal with this situation?	Level 1	6 3 2
SDK 016	Does the ins SDK do a quality check? What quality measure do you use?	Level 1	6 3 2
SDK 017	What actionable feedback does the iris SDK supply the operator (i.e., distance, motion, gaze, pupil dilation)?	Level 1	6 3 2
SDK 018	Does your Iris SDK accommodate rotation of Iris images? What degree of iris rotation does it tolerate? Is it adjustable?	Level 2	6 3 2
SDK 019	Does the iris SDK support 1 few identification?	Level 3	6 3 2
SDK 020	Does your Face SDK support feature extraction and template generation?	Level 1	6 3 3
SDK 021	Does the face SDK support auto centering, auto cropping and auto rotation correction?	Level 1	6 3 3
SDK 022	Does the face SDK include a quality check? What quality measure do you use?	Level 1	6 3 3
SDK 023	Does the face SDK support auto capture from streaming video?	Level 1	6 3 3
SDK 024	Does your Face SDK support 1. few identification?	Level 2	6 3 3
SDK 025	Did the proposed algorithm participate in the NIST slap segmentation test? Confirm that the proposed algorithm is the same or better the appropriate tests	Level 1	6 3 4

S. P. Nanavati, DDG

Identity Solutions Operating Company Private Limited

SDK 026	Has the proposed fingerprint matcher been tested in the NIST Proprietary Template Test program? Provide the results for the matcher proposed	Level 1	6.3.4
SDK 027	Did the proposed iris matching algorithm participate in the Irex tests? Provide the results and confirm that the proposed algorithm is the same or better than shown in the tests	Level 1	6.3.4
SDK 028	Does the SDK support compression/Decompression in WSQ, JPEG 2000, PNG formats with ability to specify the average compression ratio?	Level 1	6.3.4
SDK 029	Affirm that the fingerprint template of the SDK is fully compliant with standard specified in Biometric Standards for UID Applications. How is the compliance tested?	Level 1	6.3.4
SDK 030	Does the iris SDK have the capability of extracting KIND_VGA, KIND_CROPPED and KIND_CROPPED__AND_MASKED images from captured image?	Level 1	6.3.4
SDK 031	Does the iris SDK have the capability of creating and storing iris templates from KIND_VGA, KIND_CROPPED and KIND_CROPPED_AND_MASKED images?	Level 1	6.3.4
SDK 032	Does the iris SDK have the ability to read and write to a variety of industry standard image formats including PNG, JPEG 2000 and BMP?	Level 1	6.3.4
SDK 033	Does your FP SDK support ISO/IEC 19794-2 2005 compliant template extraction and matching, both without using extended data?	Level 1	6.3.4
SDK 034	Does your FP SDK have the ability to handle a variety of industry standard image formats including PNG, WSQ and BMP?	Level 1	6.3.4
SDK 035	Can your Face SDK handle a variety of industry standard image formats, including PNG, JPEG 2000 and BMP?	Level 1	6.3.4
SDK 036	Does your SDK support image conversion between BMP, RAW, JPEG, JPEG 2000, PNG formats?	Level 2	6.3.4
SDK 037	How does your face SDK check for compliance with ISO standards?	Level 2	6.3.4
SDK 038	Does your SDK function correctly on all platforms without hanging or memory leaks over a long period of time?	Level 1	6.3.5
SDK 039	Does the SDK communicate only with the application software without directly accessing any additional resources such as H/W, file or network?	Level 1	6.3.6
SDK 040	Does your SDK work without a dongle or key license during operation?	Level 1	6.3.7
SDK 041	Confirm that the API of the SDK is in pure C (not C++) and that it does not differ between the Windows and Linux versions	Level 2	6.3.7
SDK 042	Does your SDK provide a compact, and easy to use interface without conditional compilations for different platforms?	Level 2	6.3.7
SDK 043	Is the SDK provided a single one for all the modalities or separate one for each modality?	Level 3	6.3.7
SDK 044	Does your SDK support Linux (X86)? Does it have 32 & 64 bit support? Specify the certified Linux platforms that are supported	Level 1	6.3.8
SDK 045	Does your SDK support Windows XP & Above? Does it support 32 & 64 bit processors?	Level 1	6.3.8

L-1 Identity Solutions Operating Company Private Limited

Annexure VI.a.3

Guidance on Requirement Level	
Level 1	There is no option. The system must accomplish the task as stated in the top level specification. Solution provider must figure out how to comply with the requirement.
Level 2	Next requirement or degree level down from Level 1, stating there is no option, however if there is risk associated with the requirement, then the contractor can, if problems occur, apply to mitigate the requirement by following an alternative development option.
Level 3	Next requirement or specified degree level down from Level 2, stating that there are options within the latitude of the designer. If during analysis, the contractor and users find a better way of implementing a requirement and is a suitable variation of what was called for in the requirement.
Level 4	Means optional. This is a nice to have requirement or specification, but is optional.

Technical Particulars	
1	Bidder shall supply, install & commission the required hardware for succesful deployment of the solution. Sections VI.b provides the minimum requirements of some of the hardware components including the storage devices that the Bidder shall comply with
2	The Bidder must supply, install & commission the hardware at both Primary and BCP sites .
3	Section VI.c provides the list of system and other softwares that the Bidder shall include as part of the black box ABIS solution offered. The Bidder shall comply with the stated minimum requirements for the softwares mentioned The Bidder shall factor the associated costs as part of the unit price per transaction for de-duplication

M. P. Nanavati, DDG

L-1 Identity Solutions Operating Company Private Limited

Annexure VI.b.1 (i)

Blade Servers

Sr. No.	Parameter	Minimum Requirements	Unit of Measurement
1	Power Specification	Indian power specifications in terms of Phase, Voltage, Freq	Ø,V,Hz
	No. of Processors proposed	2	No CPU/Sockets in one server, can have more cpus in a single blade
	No of cores in each processor	6	No of cores in each physical CPU/socket
	Processor Type (CISC, EPIC, RISC)	x86	CISC / EPIC / RISC
	Type of processor	64-bit	32-bit / 64-bit
	Native support for 32-bit applications	YES	YES/NO
2	Architecture		
	64-bit architecture	YES	YES/NO
3	Main Memory		
	Proposed Memory size	64	GB
	Proposed Main Memory Type	DDR2	(DDR2 / DDR3)
	Main Memory Type	ECC	(ECC / Non ECC)
4	Disk Controller		
	RAID protection type proposed	RAID 0	YES / NO
	No. of channels in the proposed RAID controller	Single	Single / Dual / Quad
	Proposed size of battery backed cache	128 MB	MB
5	Internal Disks		
	Type of disk proposed	SAS/SATA	YES / NO
	Disk capacity	73 GB	GB
	Are Proposed Disks Hot Swappable?	YES	YES / NO
	Max. no of Disks supported in the proposed server	2	
6	CD / DVD Drive		
	No. of drives proposed	1	
	Is drive writeable / re-writeable?	NO	YES / NO
7	Network		
	Type of Ethernet controller proposed	Full duplex 1 /10 Gbps	YES / NO
	No of Ethernet Controllers proposed	2	Units
	Dual Homing proposed	YES	YES / NO
	Teaming of Ethernet Controllers proposed	YES	YES / NO
	Total Throughput of all the proposed Ethernet Controllers together		Gbps
	TCP/IP offload engine		YES / NO
8	Host based Adapters		
	Type of HBA proposed	Full duplex Fiber channel	
	Throughput of each of the proposed HBA	4/8 Gbps	Gbps
	Proposed HBA		PCI / PCI-X

Annexure VI.b.1 (i)

Blade Servers

Sr. No	Parameter	Minimum Requirements	Unit of Measurement
	I/O Slot used by HBA		PCI / PCI-X
	No. of HBA proposed	2	Units
	No. of ports on each HBA proposed	Dual	Single / Dual / Quad
	Whether only single port is be used on each controller	Yes	YES / NO
	Total Throughput of all the proposed HBA together		Gbps
	Capability to dynamically load balance between multiple HBA	YES	YES / NO
	Support for storage subsystems of leading manufacturers like EMC, Hitachi, HP, IBM, SUN etc.	YES	YES / NO
	LUN Size	10	in TB
	No of LUNs		Max luns supported per server
9	Power Supply		
	Hot Swappable Power supply proposed	YES	YES / NO
	(N+N) redundant power supply proposed	YES	YES / NO
	Dual AC input proposed	YES	YES / NO
10	Cooling Fans		
	Hot Swappable Cooling Fans proposed	YES	YES / NO
11	Operating System		
	Operating Systems proposed on this server	Linux	Redhat/Suse/Others, edition
	Operating system is natively compliant with 32-bit and 64-bit applications	YES	YES / NO
12	File System		
	Maximum file system partition size (file system)	8	TB
13	Support		
	Is the proposed product/solution End-of-life or will reach End-of-life within 24 months from the date of submission of bid or 12 months from the date of acceptance, whichever is later?	NO	YES / NO
	Will the proposed product/solution reach End-of-support during the currency of contract?	NO	YES / NO

D.P. Nanawati, DDG

L-1 Identity Solutions Operating Company Private Limited

Annexure VI.b.1 (ii)

Blade Servers Chassis

Sr. No	Paramoter	Minimum Requirements	Unit of Measurement
1	Power Specification	Indian power specifications in terms of Phase, Voltage, Freq	Ø,V,Hz
	Backplane redundancy	YES	YES/NO - dual backplane bus for high availability
	Number of 10G Ethernet ports - from chassis to external network	2	
	High Availability for 10 G ethernet	YES	
	Number of 1G Ethernet ports - from chassis to external network	2	
	High Availability for 1 G ethernet	YES	
	Number of Fiberchannel ports (4/8 Gbps) from chassis to external network	4	
	High Availability for FC ports	YES	
	Hot Swappable Power supply proposed	YES	YES / NO
	Dual AC input proposed	YES	YES / NO
2	Support		
	Is the proposed product/solution **End-of-life** or will reach **End-of-life** within 24 months from the date of submission of bid or 12 months from the date of acceptance, whichever is later?	NO	YES / NO
	Will the proposed product/solution reach **End-of-support** during the currency of contract?	NO	YES / NO

Private Limited * L-1 Identity Solvable Operating Company

Annexure VI.b.2 (i)

SAN

Sr. No	Parameter	Minimum Requirement	Unit of Measurement
1	Power Specification	Indian power specifications in terms of Phase, Voltage, Freq	Ø,V,Hz
2.	Proposed usable capacity of SAN storage array	10	TB
	Support for Global hot spare disks	YES	YES / NO
	Are Proposed Disks Hot Swappable?	YES	YES / NO
	Capability for Online storage expansion without reboot	YES	YES / NO
	Capability of completely automating activities, including but not limited to, defrag routines scan disks, disk scrubbing, file system checks, consistency checks, etc	YES	YES / NO
3	Controllers		
	Hardware based storage RAID controller	YES	YES / NO
	Hot swappable controller cards?	YES	YES / NO
	Type of RAID protection supported	6+1	RAID 0, 1, 5, 1+0, 6+1
	Throughput of each FC port	4 Gbps	4/8 Gbps
	Storage system end-to-end bandwidth from FC host port to backend disk	4 Gbps	4/8 Gbps
4	FC-AL loop		
	Bandwidth of FC-AL loop	4 Gbps	4/8 Gbps
5	Cache		
	Type of proposed Control Cache	ECC	ECC / Non-ECC
	Type of proposed Data Cache	ECC	ECC / Non-ECC
	Is Data Cache board hot swappable?	YES	YES / NO
	Is Control Cache board hot swappable?	YES	YES / NO
	Will the proposed product/solution reach **End-of-support** during the currency of contract?	NO	YES / NO

D.P. Nanavati, DSC

L-1 Identity Solutions Operating Company Private Limited

Annexure VI.b.3

Rack Server

Sr. No	Parameter	Minimum Requirements	Unit of Measurement
1	Power Specification	Indian power specifications in terms of Phase, Voltage, Freq	Ø,V,Hz
2	Processor		
	Processor Type (CISC, EPIC, RISC)	x86	CISC / EPIC / RISC
	Type of processor	64-bit	32-bit / 64-bit
	Native support for 32-bit applications	YES	YES/NO
3	Architecture		
	64-bit architecture	YES	YES/NO
4	Main Memory		
	Main Memory Type	ECC	(ECC / Non ECC)
5	Disk Controller		
	RAID protection type proposed	RAID 1	YES / NO
	No of channels in the proposed RAID controller	Single	Single / Dual / Quad
	Proposed size of battery backed cache	128 MB	MB
6	Internal Disks		
	Type of disk proposed	SAS/SATA/Other	YES / NO
	Disk capacity	73 GB	GB
	Disk Speed	15000 RPM	RPM
	Are Proposed Disks Hot Swappable?	YES	YES / NO
7	Network		PCI / PCI-X
	Type of Ethernet controller proposed	Full duplex 10/100/1000 Mbps	Units
	No of ports used on each Ethernet controller proposed	Single	YES / NO
	Whether only single port is be used on each controller	Yes	YES / NO
	Dual Homing proposed	YES	Gbps
	Teaming of Ethernet Controllers proposed	YES	YES / NO
	No of 10 G Ethernet ports	2	
	No of 1 G Ethernet ports	2	
8	Host based Adapters		Gbps
	Type of HBA proposed	Full duplex Fiber channel	PCI / PCI-X
	Throughput of each of the proposed HBA	4/8 Gbps	PCI / PCI-X
	No of HBA proposed	2	YES / NO
	No of ports used on each HBA proposed	Single	Gbps
	Whether only single port is be used on each controller	Yes	YES / NO
	Capability to dynamically load balance between multiple HBA	YES	
	Support for storage subsystems of leading manufacturers like EMC, Hitachi, HP, IBM, SUN etc	YES	YES / NO
9	Power Supply		YES / NO
	Hot Swappable Power supply proposed	YES	YES / NO
	(N+1) redundant power supply proposed	YES	
	Dual AC input proposed	YES	YES / NO
10	Cooling Fans		YES / NO
	Hot Swappable Cooling Fans proposed	YES	

Identity Solutions Operated by Accenture Private Limited

Annexure VI.b.3

Rack Server

Sr. No	Parameter	Minimum Requirements	Unit of Measurement
	(N+1) redundant Cooling Fans proposed	YES	
11	File System		
	Is the file system proposed a Cluster File System	YES	
	Does the file system support Journaling	YES	
28	Support		
	Is the proposed product/solution **End-of-life** or will reach **End-of-life** within 24 months from the date of submission of bid or 12 months from the date of acceptance, whichever is later?	NO	
	Will the proposed product/solution reach **End-of-support** during the currency of contract?	NO	
30	Remote Management	YES	

B.P. Nanawati, DDG

L-1 Identity Solutions